Universidad de Cantabria

Facultad de Ciencias

DISEÑOS COMBINATORIOS

Combinatorial designs

Trabajo de Fin de Grado
para acceder al
GRADO DE MATEMÁTICAS

Autora: **Raquel Pérez Martín**
Director: **Daniel Sadornil Renedo**

Junio 2021

Agradecimientos

A mi tutor, Daniel Sadornil. Por la paciencia que ha tenido conmigo durante estos cuatro años y su inestimable ayuda siempre que lo he necesitado, especialmente en la realización de este trabajo. Ha sido un placer tenerle como profesor y tutor.

También me gustaría agradecer la ayuda de Cecilia Pola, su buena disposición en la realización de un algoritmo para este proyecto y el buen trato recibido por su parte.

En general, gracias a todos y a cada uno de los profesores que me han dado clase durante este tiempo, de todos vosotros he aprendido algo que me ha hecho crecer personal y profesionalmente.

No me olvido de Emilio, mi profesor de Matemáticas de Secundaria. Su extraordinaria labor como docente y sobre todo, como persona, han hecho que esté acabando esta carrera con el objetivo de ser tan buena profesora de matemáticas como lo ha sido él.

A toda mi familia. A mi madre Cristina, a mi padre Fernando y a mis hermanas Laura y Henar, sin su apoyo constante e incondicional no habría llegado hasta aquí. En especial, quiero dedicar este trabajo a mis abuelos; Agustín, Martina, Miguel y María Jesús. Sé que están y estarían muy orgullosos de mí.

A mis amigos y a todos mis compañeros que han seguido este camino conmigo. Les agradezco infinitamente su apoyo, ayuda y compañía. Ellos han hecho que los malos momentos fuesen más amenos.

Resumen

La teoría del diseño combinatorio tiene sus orígenes en la teoría estadística del diseño experimental, en la geometría e incluso en las matematicas recreativas durante los siglos XVIII y XIX. Es una parte de la matemática combinatoria que estudia la existencia y construcción de subconjuntos de un conjunto finito, de forma que se satisfagan propiedades de equilibrio y/o simetría.

Un importante objetivo del estudio de diseños combinatorios es comprobar la existencia de los mismos cuando están sujetos a ciertas condiciones, así como determinar si son únicos o si poseen solución. Para el estudio de los diseños combinatorios se utilizan herramientas de álgebra lineal, de grupos, de cuerpos finitos y, sobre todo, de la combinatoria.

En este trabajo se estudiarán las nociones básicas y propiedades de los diseños combinatorios, incluyendo resultados de existencia, diseños sujetos a distintas propiedades y algunas construcciones de los mismos.

Palabras clave: Teoría de diseños combinatorios, diseño de experimentos, sistemas de Steiner, Cuadrados Latinos.

Abstract

Combinatorial design theory has its origins in the statistical theory of experimental design, in geometry and even in recreational mathematics during the 18th and 19th centuries. It is a part of combinatorial mathematics that studies the existence and construction of subsets of a finite set, so that balance and/or symmetry properties are satisfied.

An important objective of the study of combinatorial designs is to prove their existence when they are subject to certain conditions, as well as to determine whether they are unique or they have a solution. Tools from linear algebra, groups, finite fields and, above all, combinatorics are used to study combinatorial designs.

This paper aims to show the basic notions and properties of combinatorial designs, including existence results, designs subject to different properties and some constructions of them.

Keywords: Combinatorial design theory, experimental design, Steiner systems, Latin Squares.

Índice general

Introducción

Supongamos que queremos organizar distintas actividades con nueve niños durante cuatro días, de manera que cada día se realice, por grupos de tres, un taller distinto. Como el objetivo es que todos los niños aprendan y se conozcan entre sí, debemos organizar diferentes grupos cada día de forma que cada par de niños solo coincida en un grupo un único día. Además, todos los niños han de realizar todos los días la actividad correspondiente, es decir, a lo largo de esos días cada niño formará parte de cuatro grupos distintos.

Del mismo modo, supongamos que una compañía de cosméticos ha lanzado nuevos productos de limpieza facial al mercado. Dicha empresa quiere realizar un estudio que compare la eficacia de estos productos sobre la piel de los clientes. Por ello, si realizamos el estudio con v modelos distintos, queremos que cada persona pruebe el mismo número de modelos, k, y a su vez, que cada modelo sea probado por el mismo número de personas, r.

Estos problemas, entre muchos otros, son los que pretende resolver la teoría del diseño combinatorio. En particular, si identificamos a los niños o a los cosméticos como elementos y a los grupos o clientes como bloques, podemos identificar el problema como un diseño combinatorio. En este trabajo veremos que aunque estos ejemplos poseen solución, no siempre será posible encontrarla.

Los diseños resolubles son muy útiles en el diseño experimental. Un ejemplo familiar de un diseño que se puede resolver surge a la hora de crear la lista de partidos de tenis. Podemos suponer que en un torneo juegan $2n$ participantes y cada uno debe jugar exactamente una vez contra todos los demás jugadores. Además, los torneos se organizarán durante $2n-1$ días, de modo que todos los días cada participante juegue contra su respectivo contrincante, sin coincidir ambos más de una vez. Así, la lista de partidos no es más que un diseño que se puede resolver.

A medida que avance el trabajo iremos viendo las posibles soluciones a estos problemas que acabamos de plantear, pero antes necesitamos conocer algunas nociones previas sobre diseños. Comencemos dando la definición de la teoría del diseño combinatorio y el contexto histórico en el que está situado.

La teoría del diseño combinatorio es la parte de la matemática combinatoria que estudia la existencia y construcción de una familia de subconjuntos de un conjunto finito de modo que se satisfagan ciertas propiedades de equilibrio y/o simetría. Utiliza herramientas de álgebra lineal, grupos, anillos, cuerpos y sobre todo, de la combinatoria. Los conceptos básicos de la teoría del diseño son bastantes simples, pero las matemáticas que se utilizan para estudiar los diseños son variadas y muy amplias.

Tiene sus orígenes en la teoría estadística del diseño experimental, la geometría e incluso en las matemáticas recreativas durante los siglos XVIII y XIX. Han sido muchos los matemáticos que se adentraron en el estudio de los diseños combinatorios y gracias a ellos disponemos de importantes resultados acerca de estos. En particular, cabe destacar las contribuciones históricas de Euler (1707-1783), Thomas Kirkman (1806-1895), Jakob Steiner (1796-1863), Robert Lee Moore (1882-1974), Raj Cahndra Bose (1901-1987) y Wilson (1741-1793), entre muchos otros (se puede ver, por ejemplo, [7]).

El estudio de los primeros diseños se remonta a hace unos trescientos años. En 1776, en el artículo *"De Quadratis Magicis"*, Euler [12] construyó los primeros cuadrados latinos ortogonales de órdenes tres, cuatro y cinco. Dos años más tarde, planteó el mismo problema para cuadrados latinos de orden seis. Este problema es conocido como *"Euler's 36 Officers Problem"* [13], para el cual Euler no encontró ninguna solución.

En 1847, Kirkman comenzó a estudiar los sistemas que hoy denominamos sistemas de Steiner a partir de un problema planteado por Woolhouse [25] en el Diario de la dama y el caballero. En él se pedía determinar el número de posibles combinaciones de $k-$subconjuntos que se podían obtener de un conjunto con v elementos, de forma que todo $t-$subconjunto no apareciera en dos bloques distintos. Además, en 1850 Kirkman [17] demostró uno de los problemas más famosos en este campo de los diseños combinatorios y en las matemáticas recreativas; *"The 15 schoolgirl problem"*. Este problema fue planteado por él mismo como consulta número VI del Diario de la dama y el caballero. Decía así:

"Quince señoritas de una escuela caminan de tres en tres durante siete días seguidos. Es necesario organizarlas diariamente para que no haya dos de ellas que caminen juntas más de una vez en la misma semana."

A pesar de que fue Kirkman quién impulsó el estudio sobre estos diseños, llevan el nombre de Steiner [21] debido a que este, en 1853 y aparentemente sin conocer el trabajo de Kirkman, probó la existencia de los mismos. No obstante, el nombre de Kirkman está asociado a aquellos sistemas de Steiner que poseen solución.

Otra de las grandes contribuciones a la teoría de los diseños se produjo en 1938 gracias al trabajo de Fisher y Yates [15]. Ambos publicaron el libro *"Statistical Tables for Biological, Agricultural and Medical Research"*, basado en la aplicación de la teoría estadística a la agricultura y el diseño de experimentos. En él se consideraban colecciones de subconjuntos de un conjunto de forma que se cumplieran ciertas propiedades de equilibrio. El trabajo de ambos hizo que creciera el interés en esta materia y en 1939 Bose [5] publicó un artículo en el que trataba el estudio de los diseños de bloques balanceados utilizando cuerpos finitos, geometría proyectiva y métodos de diferencias para crear una infinidad de familias de diseños. Por este motivo, se suele decir que el estudio moderno de los diseños de bloques balanceados empezó con la publicación del artículo de Fisher y Yates.

El estudio de la teoría del diseño como disciplina matemática, independientemente de la combinatoria, se inició en el siglo XX con sus propios objetivos, métodos y problemas.

Las aplicaciones de los diseños combinatorios se encuentran en muchas áreas, por ejemplo, en la geometría finita, programación de torneos, loterías, criptografía, el diseño y análisis de algoritmos o en el diseño de experimentos, entre otros muchos. (ver, por ejemplo, [22] Capítulo 11 , [24] Capítulo 16)

Este trabajo de fin de grado se divide en tres capítulos. En el primero se definen los conceptos básicos relacionados con los diseños y las principales propiedades que estos poseen. Además, veremos que pueden existir diseños distintos no isomorfos con los mismos parámetros o que no siempre es posible determinar la unicidad de un diseño. En el segundo capítulo abordaremos un caso particular de los diseños combinatorios, los $t-$diseños. Estos no son más que los diseños presentados en el primer capítulo pero que satisfacen una condición adicional. En el tercer capítulo mostraremos algunas construcciones de los diseños explicados anteriormente utilizando distintas herramientas, como son los métodos de Skolem, el método de diferencias, las matrices de Hadamard o geometría afín. Finalmente, en el Anexo se muestra una pequeña introducción a los Cuadrados Latinos, que están estrechamente relacionados con los diseños combinatorios.

Capítulo 1

Algunos conceptos básicos sobre diseños

1.1. Definición y propiedades

Este capítulo está destinado principalmente a familiarizarnos con las nociones básicas de la teoría del diseño. Para ello introduciremos los primeros conceptos y propiedades sobre los diseños combinatorios, las matrices de incidencia asociadas a estos y el concepto de isomorfismo entre diseños. Se han seguido las referencias [3], [9], [22] y [24].

Definición 1.1 *Un diseño combinatorio es un par $D = (X, B)$ formado por un conjunto de elementos $X = \{x_1, x_2, ..., x_v\}$ y una familia de subconjuntos de dichos elementos $B = \{B_1, B_2, ..., B_b\}$ llamados bloques del diseño.*

La definición anterior no muestra ninguna condición sobre los bloques que forman el diseño. Es, por tanto, la definición más general de diseño combinatorio la cual incluye todos los casos posibles.
Veamos a continuación algunos diseños que más adelante clasificaremos.

Ejemplo 1 *Sea el diseño $D = (X, B)$ con $X = \{1, 2, ..., 6\}$ y el conjunto B formado por los bloques:*

$$B_1 = \{1, 2, 3\}, \quad B_2 = \{1, 5, 6\}, \quad B_3 = \{2, 3, 4\},$$

$$B_4 = \{4, 5, 6\}, \quad B_5 = \{2, 4, 5\}, \quad B_6 = \{1, 3, 6\}.$$

Ejemplo 2 *Sea el diseño $D = (X, B)$ con $X = \{1, 2, ..., 6\}$ y el conjunto B formado por los bloques:*

$$B_1 = \{1, 2, 5\}, \quad B_2 = \{2, 3, 5, 6\}, \quad B_3 = \{1, 4, 6\}, \quad B_4 = \{3, 4\}.$$

Se observa a simple vista que ambos diseños son diferentes a pesar de tener el mismo conjunto de elementos. Los diseños pueden estar sujetos a distintas restricciones y podemos clasificarlos de la siguiente forma.

Definición 1.2 *Consideremos el diseño $D = (X, B)$, entonces:*

- *Se dice que el diseño es simple si no contiene bloques iguales.*
- *Se dice que el diseño es incompleto si no existe ningún bloque que contenga todos los elementos de X.*
- *Se dice que el diseño es regular de índice r o $r-$regular, si cada elemento x_i de X pertenece al mismo número de bloques.*

- *Se dice que el diseño es uniforme de índice k o $k-$uniforme, si todos los bloques tienen el mismo número de elementos.*
- *Se dice que el diseño es simétrico si tiene tantos bloques como elementos.*

El ejemplo 1 es, por tanto, un diseño simple e incompleto, ya que todos los bloques son distintos y de tamaño tres. Por este mismo motivo también es uniforme. Además, podemos observar que cada elemento de X pertenece al mismo número de bloques; $r = 3$, luego es $3-$regular. Por último, el diseño está formado por 6 elementos y 6 bloques, siendo así simétrico.

Sin embargo, observamos que el ejemplo 2 es simple, incompleto y regular pero no es uniforme. No todos los bloques contienen el mismo número de elementos, $|B_1| = |B_3| = 3$, $|B_2| = 4$ y $|B_4| = 2$. Además, tampoco es simétrico. El diseño está formado por 6 elementos y 4 bloques.

Aunque en general los diseños con los que se suele trabajar son regulares y uniformes, existen diseños regulares no uniformes, como muestra el ejemplo 2, y diseños uniformes no regulares. Veamos más ejemplos tomando siempre el conjunto $X = \{1, 2, ..., 6\}$.

Ejemplo 3 *Sea el diseño $D = (X, B)$ con el conjunto B formado por los bloques:*

$$B_1 = \{1, 2, 5\}, \quad B_2 = \{1, 3, 6\}, \quad B_3 = \{4, 5, 6\}, \quad B_4 = \{2, 5, 6\}.$$

Podemos observar que todos los bloques son del mismo tamaño, es decir, contienen el mismo número de elementos de X, pero cada elemento de este conjunto no pertenece al mismo número de bloques. Por ejemplo, el elemento 1 pertenece a los bloques B_1 y B_2 y el elemento 3 solo pertenece al bloque B_2. Por lo tanto, es un diseño $3-$uniforme pero no regular.

Ejemplo 4 *Sea el diseño $D = (X, B)$ con el conjunto B formado por los bloques:*

$$B_1 = \{1, 3, 4\}, \quad B_2 = \{1, 6\}, \quad B_3 = \{2, 4, 5\}, \quad B_4 = \{1, 3, 5, 6\}.$$

Es un diseño no uniforme y no regular. No todos los bloques son del mismo tamaño,

$$|B_1| = |B_3| = 3, \quad |B_2| = 2 \quad y \quad |B_4| = 4,$$

y no todos los elementos de X pertenecen al mismo número de bloques. El elemento 1 pertenece a los bloques B_1, B_2 y B_4, mientras que el elemento 2 solo pertenece al bloque B_3.

En general, y salvo que se diga lo contrario, trabajaremos con diseños simples uniformes y regulares. Por ello y con el objetivo de facilitar la lectura, podemos denotar los parámetros de un diseño de la forma (v, k, r), donde k es el número de elementos que contiene cada bloque (uniformidad del diseño) y r es el número de bloques a los que pertenece cada elemento (regularidad del diseño). Esta es la definición de diseño combinatorio que aparece en la mayoría de fuentes, la cual obliga a que este sea regular y uniforme. Como ya hemos mencionado, la definición 1.1 es la más general posible. Los parámetros de uniformidad y regularidad de un diseño están relacionados entre sí, con el número de elementos y con el número de bloques del mismo, como se muestra a continuación.

Teorema 1.3 *En todo diseño de parámetros (v, k, r) y b bloques, se cumple:*

$$bk = rv.$$

Demostración: Sea (X, B) un diseño con $|X| = v$. Consideremos el conjunto $Y = \{(x, B_i)$ tal que $x \in X, B_i \in B$ y $x \in B_i\}$, es decir, el conjunto de todos los pares ordenados (x, B_i) de forma que el elemento x pertenezca al bloque B_i. Queremos ver que $bk = |Y| = rv$.

Por ser un diseño uniforme, sabemos que cada bloque B_i tiene el mismo número de elementos; k. Como $|B| = b$, hay b opciones de elegir un bloque $B_i \in B$ y, para cada bloque, hay k opciones de elegir un elemento $x \in B_i$. Así, hay $b \cdot k$ pares ordenados (x, B_i) distintos, es decir, $|Y| = bk$.

Por otro lado, por ser un diseño regular, cada elemento $x \in X$ pertenece al mismo número de bloques; r. Como $|X| = v$ y para cada elemento $x \in X$ hay r bloques B_i tal que $x \in B_i$, en total hay $v \cdot r$ pares ordenados (x, B_i) distintos, esto es, $|Y| = vr$.

Entonces se cumple que $|Y| = bk$ y $|Y| = vr$ y, en consecuencia, $bk = rv$. □

Este teorema proporciona una condición necesaria para la existencia de un diseño. En particular, si (v, k, r) es un diseño, se tiene $k \mid vr$. Con el objetivo de que esta condición también sea suficiente y podamos garantizar la existencia de un diseño, es necesario añadir otra relación entre los parámetros. Sabemos que el número de subconjuntos de X de tamaño k es $\binom{v}{k}$, luego el número de bloques del diseño no puede superar, lógicamente, ese número.

$$b = \frac{vr}{k} \leq \binom{v}{k}.$$

Esta será la relación adicional que deben cumplir los parámetros de un diseño para que la condición anterior sea también suficiente.

Teorema 1.4 (Teorema de existencia de diseños combinatorios) *Existe un diseño de parámetros (v, k, r) sí, y solo sí,*

$$bk = rv \quad y \quad b \leq \binom{v}{k}.$$

Demostración: La condición de necesidad está probada en el teorema 1.3 y en el párrafo anterior a este. Veamos que esta condición es suficiente.

Consideremos el conjunto X con $|X| = v$. Sea P_k el conjunto de todos los subconjuntos de tamaño k de X y sea $C = \{B_1, B_2, ..., B_b\}$ un conjunto formado por b bloques tal que en cada bloque haya k elementos. Claramente, el conjunto C está contenido en P_k. Por tanto, por la definición 1.2, el conjunto C es uniforme.
Ahora, para cada elemento $x \in X$, definimos $r(x)$ como el número de bloques a los que pertenece el elemento x de X. Por la condición de uniformidad y como, por hipótesis $b = \frac{vr}{k}$, se cumple que

$$\sum_{x \in X} r(x) = bk = vr. \tag{1.1}$$

Si $r(x) = r$ para todo elemento $x \in X$, entonces se cumple que C es un diseño $r-$regular con parámetros (v, k, r) y ya habríamos acabado.
En caso contrario, existe al menos un elemento $x^{'}$ tal que $r(x^{'}) \neq r$, es decir, $r(x^{'}) = r^{'}$. Entonces, para que se cumpla la ecuación (1.1) se deduce que si $r^{'}$ es menor que r, ha de existir un elemento $x^{''}$ en X con $r(x^{''}) = r^{''} > r$, y si $r^{'}$ es mayor que r, ha de existir un elemento $x^{''}$ con $r(x^{''}) = r^{''} < r$. En este caso, C no es un diseño ya que no se cumple la regularidad.

Supongamos que x_1 es un elemento de X que aparece en más de r bloques y x_2 un elemento que aparece

en menos. Sea n_{12} el número de bloques de C que contienen a x_1 y no a x_2, n_{21} el número de bloques de C que contienen a x_2 pero no a x_1 y n el número de bloques que contienen a ambos elementos. Entonces, se cumple que

$$n_{12} = r(x_1) - n \geqslant 0 \quad y \quad n_{21} = r(x_2) - n \geqslant 0 \tag{1.2}$$

y, por tanto,

$$n_{12} - n_{21} = r(x_1) - r(x_2) > 0, \tag{1.3}$$

ya que el elemento x_1 aparece en más bloques que el elemento x_2. De la ecuación (1.3) obtenemos que $n_{12} > n_{21}$ y por la ecuación (1.2) sabemos que $n_{21} \geqslant 0$, luego n_{12} es mayor o igual que 1. Es decir, existe al menos un bloque B_i en C que contiene a x_1 pero no contiene a x_2.
Sea B_{i_0} uno de ellos. Construyamos el bloque $B^*_{i_0} = (B_{i_0} \backslash \{x_1\}) \cup \{x_2\}$ y el conjunto $C^* = (C \backslash B_{i_0}) \cup B^*_{i_0}$. Así, $C^* = \{B_1, B_2, ..., B^*_{i_0}, ..., B_b\}$ con $|C^*| = b$ y $|B_i| = k$ para todo bloque B_i contenido en C^*, y tal que

$$r^*(x_1) = r(x_1) - 1 \quad y \quad r^*(x_2) = r(x_2) + 1 \tag{1.4}$$

Si $r^*(x_1) = r = r^*(x_2)$, entonces C^* se aproximaría más a ser un diseño $r-$regular, ya que los elementos x_1 y x_2 están exactamente en r bloques. Si, de este modo, C^* es un diseño regular porque el resto de elementos de X aparecen todos en r bloques, habríamos acabado. De lo contrario, continuamos con el mismo proceso un número finito de veces hasta que los números $r^*(x_1)$ y $r^*(x_2)$ sean iguales a r.

Repitiendo este proceso con los elementos x_i y x_j que no cumplan la regularidad del diseño, obtendremos que $r^*(x_i)$ y $r^*(x_j)$ difieren cada vez menos de r hasta ser iguales a dicha constante y así, conseguir un diseño $r-$regular. □

Observamos que esta demostración además nos permite, dado un diseño uniforme, obtener la regularidad del diseño cambiando los elementos de sus bloques. Veamos si pueden existir los diseños propuestos en el siguiente ejemplo.

Ejemplo 5 *Ejemplos de diseños:*

I) *Diseño de parámetros* $(6, 3, 1)$. *En este caso se cumple que* $3 \mid 6 \quad y \quad 2 \leq \binom{6}{3}$, *luego existen diseños con esos parámetros. Uno de ellos podría estar formado, por ejemplo, por el conjunto de bloques* $B = \{\{1, 2, 3\}, \{4, 5, 6\}\}$.

II) *Diseño de parámetros* $(5, 2, 1)$. *Podemos observar que* 2 *no divide a* 5, *luego no existe ningún diseño con estos parámetros.*

III) *Diseño de parámetros* $(7, 3, 3)$. *Se cumple que* $3 \mid 21 \quad y \quad 7 \leq \binom{7}{3}$, *y por tanto, existirá al menos un diseño con esos parámetros. En particular, dado el diseño formado por el conjunto de bloques:*

$$B_1 = \{1, 2, 3\}, \quad B_2 = \{1, 2, 4\}, \quad B_3 = \{1, 2, 5\}, \quad B_4 = \{1, 2, 6\},$$

$$B_5 = \{3, 5, 6\}, \quad B_6 = \{4, 6, 7\} \quad y \quad B_7 = \{2, 3, 7\},$$

observamos que es $3-$*uniforme pero no es regular, ya que* $r(1) = 4$, $r(2) = 5$, $r(3) = 3$, $r(4) = 2$, $r(5) = 2$, $r(6) = 3$ *y* $r(7) = 2$.
Utilizando el proceso seguido en la demostración del teorema 1.4, vamos a ver que modificando los elementos de dichos bloques conseguiremos que el diseño sea $3-$*regular.*
Como $r(1) = 4$ *y* $r(4) = 2$, *cambiando el elemento* 1 *del bloque* B_1 *por el elemento* 4, *tenemos que* $r(1) = 3$ *y* $r(4) = 3$.
Observamos también que el elemento 2 *pertenece a cinco bloques y el elemento* 5 *a dos. Cambiamos*

el elemento 2 *del bloque* B_2 *por el elemento* 5. *Así,* $r(2) = 4$ *y* $r(5) = 3$.
El elemento 2 *sigue perteneciendo a cuatro bloques mientras que el elemento* 7 *solo está en dos. Intercambiamos el elemento* 2 *del bloque* B_3 *por el* 7, *obteniendo así* $r(2) = 3$ *y* $r(7) = 3$.
Los bloques modificados del diseño quedarían de la siguiente forma:

$$B_1 = \{2, 3, 4\}, \quad B_2 = \{1, 4, 5\} \quad y \quad B_3 = \{1, 5, 7\}.$$

Por lo tanto, siguiendo el procedimiento del teorema 1.4, hemos construido un diseño con parámetros $(7, 3, 3)$.

A continuación, vamos a probar que el conjunto formado por todos los posibles $k-$subconjuntos de un conjunto X determina un (v, k, r) diseño, donde el parámetro r toma un valor fijo que estará dado, lógicamente, por el resto de parámetros del diseño.

Corolario 1.5 *El conjunto de bloques formado por todos los* $k-$*subconjuntos de un conjunto* X *de tamaño* v *es un* (v, k, r) *diseño donde* $r = \binom{v-1}{k-1}$.

Demostración: Queremos probar que dado un conjunto formado por todos los posibles bloques de k elementos tomados de un conjunto X de tamaño v, es un diseño. Por definición, se cumple la uniformidad del diseño. Entonces, basta probar la regularidad, es decir, que todo elemento de X pertenece al mismo número de bloques. Dado un elemento $x \in X$ queremos ver a cuántos $k-$subconjuntos pertenece, pero es fácil observar que basta con elegir $k-1$ elementos de los $v-1$ restantes en X para formar un bloque que le contenga. De esta forma, el elemento x estará en $\binom{v-1}{k-1}$ bloques. Por tanto, todo elemento de X pertenecerá a ese número de bloques y podemos concluir que se cumple la regularidad del diseño, donde $r = \binom{v-1}{k-1}$. □

1.2. Matrices de incidencia

Acabamos de ver que dado un diseño (X, B), cada elemento del conjunto X puede pertenecer a uno o a varios bloques de B. Por ello, veremos que un diseño no es más que un sistema de incidencia que muestra la relación existente entre los elementos y los bloques que lo forman. Utilizaremos matrices para representar de forma más sencilla estos sistemas.

Definición 1.6 *Sea* (v, k, r) *un diseño. La matriz de incidencia de este diseño es una matriz* A *de tamaño* $v \times b$ *en la que cada elemento* (a_{ij}) *se define de la siguiente forma:*

$$(a_{ij}) = \begin{cases} 1 & \textit{si el elemento } x_i \textit{ pertenece al bloque } B_j \\ \\ 0 & \textit{en caso contrario} \end{cases}$$

Con esta definición obtenemos que cada elemento y cada bloque del diseño se corresponden respectivamente con una fila y con una columna de la matriz.

Además, se observa que conociendo únicamente la matriz de incidencia de un diseño podemos saber si dicho diseño es regular y/o uniforme. En efecto, si en cada fila aparece el mismo número de elementos distintos de cero, sabremos que cada elemento del diseño está contenido en el mismo número de bloques (regularidad). Y, si en cada columna aparece el mismo número de elementos distintos de cero, sabremos que cada bloque contiene el mismo número de elementos. Esto nos garantiza la uniformidad. Veamos un ejemplo.

Ejemplo 6 *Sea* $(6,3,3)$ *el diseño del ejemplo 1. La matriz de incidencia asociada a este diseño es la siguiente:*

$$A_{6\times 6} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Observamos que en cada fila aparecen tres elementos distintos de cero y que en cada columna hay también el mismo número de elementos distintos de cero. Esto significa que cada elemento pertenece al mismo número de bloques; $r = 3$*, y que todos los bloques tienen el mismo tamaño;* $k = 3$*. Luego es un diseño* $3-$*regular y* $3-$*uniforme, como ya sabíamos.*

Como ya hemos mencionado, a partir de la matriz de incidencia de un diseño podemos conocer la regularidad y uniformidad de este. Por ello, es claro que de esta relación entre la matriz de incidencia y los parámetros r y k de un diseño regular y uniforme, se puede determinar la siguiente propiedad relativa a la matriz de incidencia de todo diseño.

Proposición 1.7 *Sea* $A \in \mathcal{M}_{v\times b}(\mathbb{Z}/2\mathbb{Z})$ *la matriz de incidencia de un diseño regular y uniforme. Si* J_n *denota la matriz de tamaño* $n \times n$ *con todos los términos iguales a* 1*, entonces se cumple que* $J_v A = kJ_{v\times b}$ *y* $AJ_b = rJ_{v\times b}$*.*

Demostración: Comencemos probando la primera igualdad. Sea la matriz $M = J_v A$, entonces cada elemento m_{ij} es el producto de la fila i de J_v por la columna j de A. Sabemos que todas las filas de la matriz J_v son iguales y que, por ser A la matriz de incidencia de un diseño uniforme, todo bloque del diseño contiene al mismo número de elementos, esto es, todas las columnas de A tienen el mismo número de unos; k. Por tanto, todos los elementos m_{ij} tienen el mismo valor k y, con ello, se cumple que $J_v A = kJ_{v\times b}$.

Del mismo modo probamos la segunda igualdad. Sea la matriz $N = AJ_b$, entonces cada elemento n_{ij} es el producto de la fila i de A por la columna j de J_b. Por ser A la matriz de incidencia de un diseño regular, todo elemento pertenece al mismo número de bloques, es decir, todas las filas de A tienen el mismo número de unos; r. Como la matriz J_b tiene todas sus columnas iguales a 1, entonces todos los elementos n_{ij} tomarán el mismo valor r. Así, obtenemos que se cumple la ecuación $AJ_b = rJ_{v\times b}$. □

Hemos visto que, dado un diseño, siempre tenemos una matriz de incidencia asociada a él. Veamos ahora que es posible obtener nuevos diseños modificando la matriz de incidencia de uno dado. Por ejemplo, si calculamos la matriz traspuesta de la matriz de incidencia de un diseño, esta seguirá siendo la matriz de incidencia de otro diseño. Al diseño resultante le denotaremos como el diseño dual del original, en el cual se intercambian los roles de elementos y bloques.

Definición 1.8 *Dado un diseño* $D = (X, B)$*, llamamos diseño dual* $D^T = (X^T, B^T)$ *de* D *al diseño en el que cada elemento* x *de* X *se corresponde con un bloque* B_i^T *de* B^T *y cada bloque* B_i *de* B *se corresponde con un elemento* x^T *de* X^T*.*

En otras palabras, un elemento $x^T \in X^T$ pertenece al bloque B_i^T de B^T sí, y solo sí, el elemento $i \in X$ pertenece al bloque B_{x^T} de B. Además, a partir de la definición es claro que el diseño dual D^T de D será un diseño de parámetros (b, r, k).

Ejemplo 7 *Sea D el diseño de parámetros $(8,4,3)$ cuyo conjunto de bloques está formado por $B = \{\{1,2,3,4\},\{5,6,7,8\},\{1,3,6,8\},\{2,3,4,7\},\{1,4,5,6\},\{2,5,7,8\}\}$.*
Observamos que el elemento 1 pertenece a los bloques B_1, B_3 y B_5, el elemento 2 a los bloques B_1, B_4 y B_6,..., etc. Entonces, el diseño dual D^T de D está formado por el conjunto de elementos $X^T = \{1,2,3,4,5,6\}$ y el siguiente conjunto de bloques:

$$B_1^T = \{1,3,5\}, \quad B_2^T = \{1,4,6\}, \quad B_3^T = \{1,3,4\}, \quad B_4^T = \{1,4,5\},$$

$$B_5^T = \{2,5,6\}, \quad B_6^T = \{2,3,5\}, \quad B_7^T = \{2,4,6\}, \quad B_8^T = \{2,3,6\}.$$

Es fácil ver que el diseño D tiene 8 elementos y 6 bloques, y su diseño dual D^T tiene 6 elementos y 8 bloques. Es decir, se han intercambiado las funciones de los elementos y bloques del diseño inicial. Por tanto, el diseño dual D^T tiene parámetros $(6,3,4)$.

Si A es la matriz de incidencia de un diseño D, entonces la matriz traspuesta A^T de A es la matriz de incidencia del diseño dual D^T de D. Con esto, claramente se tiene que el diseño dual del diseño dual es el propio diseño.

Otra forma de obtener un nuevo diseño a partir de uno dado es el que se obtiene al intercambiar los elementos iguales a 1 por 0 en la matriz A de incidencia y viceversa, es decir, si reemplazamos cada bloque B_i de B por su complementario.

Definición 1.9 *Sea $D = (X,B)$ un diseño, llamamos diseño complementario $\bar{D} = (\bar{X}, \bar{B})$ de D al diseño formado por el mismo conjunto de elementos y por un conjunto de bloques que contiene a los complementarios de los bloques B_i de B.*

De este modo y como mencionábamos anteriormente, la matriz de incidencia $\bar{A}$ del diseño complementario $\bar{D}$ de D se obtiene intercambiando los elementos 0 y 1 de la matriz A.

De nuevo, a partir de la definición, el diseño complementario $\bar{D}$ tendrá los parámetros $(v, v-k, b-r)$.

Si nos fijamos en el ejemplo 7, el diseño complementario $\bar{D}$ de D está formado por $\bar{X} = X$ y por el conjunto de bloques $\bar{B} = \{\{5,6,7,8\},\{1,2,3,4\},\{2,4,5,7\},\{1,5,6,8\},\{2,3,7,8\},\{1,3,4,6\}\}$, es decir, es un $(8,4,3)$ diseño.

1.3. Isomorfismos

Sabemos que dado un diseño siempre tenemos una matriz de incidencia asociada a él, y que, a partir de dicha matriz de incidencia, podemos obtener nuevos diseños. Pero, ¿estos diseños son únicos? O mejor dicho, dados los valores v, k, r, ¿pueden existir distintos diseños con estos parámetros? Debemos aclarar que si simplemente volvemos a etiquetar los elementos o enumeramos los bloques en un orden diferente, tenemos esencialmente el mismo diseño.

Con el objetivo de resolver estas preguntas introducimos el concepto de isomorfismo. Dos diseños serán isomorfos si existe una biyección entre los conjuntos de elementos de dichos diseños y, de la misma forma, entre los conjuntos de los bloques de ambos. Si no existe esa biyección, los diseños no serán isomorfos.

Definición 1.10 *Sean $D = (X,B)$ y $D' = (X', B')$ dos diseños con $|X| = |X'|$. Se dice que son isomorfos si existe una biyección $\psi : X \longrightarrow X'$ tal que para cualquier bloque $B_i \in B$ existe $B'_j \in B'$ donde $B'_j = \{\psi(x)$ tal que $x \in B_i\}$.*

Si $D^{'} = D$, la biyección ψ es un automorfismo.

En términos de matrices de incidencia, si A y $A^{'}$ son las matrices de incidencia de los diseños D y $D^{'}$ respectivamente, es fácil ver que los diseños D y $D^{'}$ son isomorfos si se puede obtener uno a partir del otro intercambiando elementos o bloques, es decir, si podemos obtener la matriz $A^{'}$ intercambiando las filas o columnas de la matriz A. En particular, D será isomorfo a $D^{'}$ si existen matrices de permutaciones P y Q de tamaño $v \times v$ y $b \times b$ respectivamente tales que:

$$A^{'} = PAQ. \tag{1.5}$$

Ejemplo 8 *Consideremos de nuevo el diseño del ejemplo 7 de parámetros* $(8, 4, 3)$.
Sea $\psi : X \longrightarrow X^{'}$ *tal que* $\psi(1) = 7$, $\psi(3) = 5$, $\psi(2) = 4$, $\psi(6) = 8$ *y* $B_1^{'} = B_3$, $B_2^{'} = B_4$, $B_3^{'} = B_6$, $B_4^{'} = B_1$, $B_5^{'} = B_2$, $B_6^{'} = B_5$. *Entonces el diseño* $D^{'} = (X^{'}, B^{'})$ *de parámetros* $(8, 4, 3)$ *es isomorfo a* D. *Veamos cómo son las matrices de incidencia de ambos diseños:*

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad A^* = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad A^{'} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Se observa a simple vista que la matriz A^* *se obtiene intercambiando las filas de la matriz* A *que corresponden a los elementos modificados por el isomorfismo; la primera fila por la séptima, la tercera por la quinta, la segunda por la cuarta y la sexta por la octava.*
Si ahora modificamos las columnas de A^*, *es decir, cambiamos el orden de los bloques según el isomorfismo; en la primera columna colocamos la tercera, en la segunda la cuarta, en la tercera la sexta, y así sucesivamente, obtenemos la matriz* $A^{'}$.
En particular, existen matrices cuadradas P *y* Q *de tamaño* 8 *y* 6 *respectivamente, tal que:*

$$A^{'} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} = PAQ$$

Además, si A^* *es la matriz de incidencia del diseño* D^*, *está claro que los diseños* D^* *y* $D^{'}$ *se corresponden con la misma biyección* ψ, *ya que la única diferencia entre ellos es el orden de los bloques.*

En el ejemplo anterior hemos construido un diseño isomorfo a uno dado. Sin embargo, una tarea menos sencilla de realizar a simple vista es averiguar cuándo dos diseños son isomorfos. Si dados dos diseños con sus respectivas matrices de incidencia A y $A^{'}$, existen matrices P y Q tales que $A^{'} = PAQ$, dichos diseños serán isomorfos. En caso contrario, los diseños serán no isomorfos. En general no es fácil saber si dados dos diseños, estas matrices P y Q existen.

Ejemplo 9 *Sean los diseños* $D = (X, B)$ *y* $D^{'} = (X, B^{'})$ *de parámetros* $(7, 3, 6)$ *formados por el conjunto* $X = \{1, 2, 3, 4, 5, 6, 7\}$ *y los siguientes conjuntos de bloques:*

$$B = \{\{1,2,3\},\{1,2,3\},\{1,4,5\},\{1,4,6\},\{1,5,7\},\{1,6,7\},\{2,4,5\}$$
$$\{2,4,7\},\{2,5,6\},\{2,6,7\},\{3,4,6\},\{3,4,7\},\{3,5,6\},\{3,5,7\}\}$$

$$B' = \{\{1,2,3\},\{1,2,4\},\{1,3,5\},\{1,4,6\},\{1,5,7\},\{1,6,7\},\{2,3,7\}$$
$$\{2,4,5\},\{2,5,6\},\{2,6,7\},\{3,4,6\},\{3,4,7\},\{3,5,6\},\{4,5,7\}\}$$

Se observa a simple vista que el conjunto de bloques del diseño D tiene dos bloques iguales y el conjunto de bloques del diseño D' tiene todos los bloques distintos. De esta forma, es fácil ver que no puede existir un isomorfismo entre ambos conjuntos y que por tanto, existen al menos dos diseños distintos con los mismos parámetros.

Por tanto, es importante tener en cuenta que los parámetros (v,k,r) no siempre determinan unívocamente un diseño, puede haber dos o más diseños no isomorfos con los mismos parámetros.
Aunque acabamos de ver que podemos conocer, dados dos diseños, si son o no isomorfos, aún no se ha descubierto si dados los parámetros (v,k,r), se cumple que determinen un único diseño (salvo isomorfismo). A pesar de esto, se conocen algunos diseños que no son únicos así como cuántos diseños no isomorfos existen de uno dado. Por ejemplo,

i) Existe un único $(6,3,5)$ diseño (salvo isomorfismo) cuyo conjunto de bloques está formado por:

$$\{1,2,3\},\quad \{1,2,4\},\quad \{2,3,6\},\quad \{1,3,5\},\quad \{1,4,6\},$$
$$\{3,4,5\},\quad \{1,5,6\},\quad \{2,4,5\},\quad \{2,5,6\},\quad \{3,4,6\}.$$

ii) Existe un único $(7,3,3)$ diseño (salvo isomorfismo) formado por los bloques:

$$\{1,2,4\},\quad \{1,3,7\},\quad \{1,5,6\},\quad \{2,3,5\},\quad \{2,6,7\},\quad \{3,4,6\},\quad \{4,5,7\}.$$

iii) Existe un único $(9,3,4)$ diseño (salvo isomorfismo) cuyo conjunto de bloques es el siguiente:

$$\{1,2,3\},\quad \{1,4,7\},\quad \{1,5,9\},\quad \{1,6,8\},\quad \{2,4,9\},\quad \{2,5,8\},$$
$$\{2,6,7\},\quad \{3,4,8\},\quad \{3,5,7\},\quad \{3,6,9\},\quad \{4,5,6\},\quad \{7,8,9\}.$$

Por otro lado, se conoce que hay 36, 11 y 80 diseños no isomorfos con parámetros $(9,3,8)$, $(9,4,8)$ y $(15,3,7)$ respectivamente.

En la sección II.1 de la referencia [7] podemos encontrar todos estos diseños y más detalles sobre diseños que son únicos y diseños no isomorfos que comparten los mismos parámetros.

Capítulo 2

t-diseños

En el capítulo 1 hemos visto qué sucede si seleccionamos subconjuntos de un conjunto de elementos de modo que se cumplan ciertas propiedades de regularidad y uniformidad. Si a esto le añadimos la condición de que cada subconjunto de t elementos del conjunto aparezca en un número fijo de bloques, independientemente de que elementos sean, surge la idea de $t-$diseños.

En este capítulo estudiaremos los casos más importantes de $t-$diseños y los que dieron origen a la teoría de diseños; los sistemas de Steiner y los $2-$diseños, conocidos como diseños balanceados. Para ello seguiremos principalmente las referencias [1], [9], [22] y [24].

Definición 2.1 *Sean v, k, λ y t parámetros enteros tal que $1 \leq t \leq k \leq v$. Un $t-(v,k,\lambda)$ diseño es un diseño (X,B) con $|X| = v$ y $k-$uniforme de manera que cada subconjunto T contenido en X con $|T| = t$ está contenido en el mismo número λ de bloques.*

Con esta definición observamos que los (v,k,r) diseños no son más que $1-(v,k,\lambda)$ diseños donde $\lambda = r$.

Ejemplo 10 *Si recordamos el diseño del ejemplo 1, es un $1-(v,k,r)$ diseño, ya que cada elemento aparece en r bloques. En concreto, $r = 3$.*
Sin embargo, no es un $t-(v,k,\lambda)$ diseño para ningún $t > 1$. Si tomamos $t = 2$, observamos que el subconjunto formado por los elementos $\{5,6\}$ sí aparece en dos bloques distintos, B_2 y B_3, y en este caso el valor de λ sería 2. Pero otros $2-$subconjuntos como $\{1,2\}$ o el $\{4,6\}$, entre otros, solo aparecen una vez. Incluso hay algunos como el $\{3,5\}$ que no aparecen en ningún bloque.
Para $t = 3$ es claro que no es un $t-$diseño ya que todos los bloques son distintos y algunos $3-$subconjuntos como, por ejemplo, el $\{3,5,6\}$ no aparecen en el diseño.

El teorema 1.3 del capítulo anterior nos da la relación que cumplen los parámetros de un (v,k,r) diseño. Veamos que esta condición no es más que un caso particular de la relación existente entre los parámetros de un $t-(v,k,\lambda)$ diseño, definida a continuación.

Teorema 2.2 *El número de bloques de un $t-(v,k,\lambda)$ diseño es*

$$b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Demostración: La demostración de este resultado es una adaptación de la demostración realizada en el teorema 1.3. Sea (X,B) un $t-(v,k,\lambda)$ diseño. Consideremos el conjunto $Y = \{(T, B_i)$ tal que $T \subset X$ con $|T| = t$ y $B_i \in B$ es un bloque con $T \subseteq B_i\}$. Queremos ver que $b\binom{k}{t} = |Y| = \lambda\binom{v}{t}$.

Por un lado, como el número de $t-$subconjuntos contenidos en un bloque B_i de tamaño k es $\binom{k}{t}$ y $|B| = b$, entonces hay $b \cdot \binom{k}{t}$ posibles pares de elementos distintos en Y.

Por otro lado, el número de $t-$subconjuntos contenidos en X con $|X| = v$ es $\binom{v}{t}$, y por definición de $t-$diseño, cada uno de ellos aparece en λ bloques B_i. Luego hay $\lambda \cdot \binom{v}{t}$ posibles pares de elementos distintos en Y.
En consecuencia, se cumple que $b\binom{k}{t} = |Y| = \lambda\binom{v}{t}$, es decir, $b = \lambda\frac{\binom{v}{t}}{\binom{k}{t}}$. □

Este teorema, al contrario que el teorema 1.4 para $1-(v,k,r)$ diseños, no garantiza la existencia de un $t-(v,k,\lambda)$ diseño. Es una condición necesaria, pero no suficiente. Veamos un contraejemplo.

Ejemplo 11 *Sea $v = 8$, $t = 2$, $k = 4$ y $\lambda = 3$, entonces por el teorema 2.2 se tiene que el número de bloques del diseño es $b = 14$. Consideremos el siguiente conjunto de bloques:*

$$\{1,2,3,4\},\quad \{5,6,7,8\},\quad \{2,4,6,8\},\quad \{1,3,5,7\},\quad \{1,4,7,8\},\quad \{3,5,6,8\},\quad \{2,3,4,7\},$$
$$\{1,2,7,8\},\quad \{1,3,5,6\},\quad \{2,5,6,7\},\quad \{3,4,5,6\},\quad \{2,6,7,8\},\quad \{1,3,7,8\},\quad \{1,2,5,6\}.$$

Se puede observar que el subconjunto $\{1,2\}$, por ejemplo, aparece en tres bloques. Sin embargo, los subconjuntos $\{7,8\}$, $\{5,6\}$ aparecen en cinco mientras que el subconjunto $\{1,4\}$ solo aparece en dos. Por tanto, como no todos los $2-$subconjuntos aparecen en el mismo número de bloques; 3, no es un $t-$diseño de parámetros $2-(8,4,3)$.

Dado un $t-$diseño, conocemos por definición el número de bloques a los que pertenece cada $t-$subconjunto del diseño; λ. Siguiendo el mismo tipo de razonamiento que en el teorema anterior, podemos conocer en cuántos bloques está cada $s-$subconjunto del conjunto X con $s \leq t$.

Teorema 2.3 *Sea (X,B) un $t-(v,k,\lambda)$ diseño y S un $s-$subconjunto contenido en X con $s \leq t$. Entonces, el número de bloques λ_s del $t-$diseño que contienen a S es:*

$$\lambda_s = \lambda\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

Demostración: Sea (X,B) un $t-(v,k,\lambda)$ diseño. Consideremos a S un $s-$subconjunto de X y sea el conjunto $Y = \{(T,B_i)$ tal que $S \subseteq T \subseteq X$ con $|T| = t$ y $B_i \in B$ es un bloque con $T \subset B_i\}$. Queremos ver que $\lambda_s\binom{k-s}{t-s} = |Y| = \lambda\binom{v-s}{t-s}$, es decir, que el número de bloques a los que pertenece el conjunto S no depende de dicho conjunto en particular, sino de su cardinal, que siempre es el mismo y que satisface la ecuación anterior.

Sea λ_S el número de bloques B_i que contienen al subconjunto S. Para conocer cuántos pares hay de la forma (T,B_i), basta ver cuántos $t-$subconjuntos contenidos en B_i contienen a S. Como S está contenido en B_i con $|B_i| = k$ y en T, solo hay $(k-s)$ opciones de elegir los $(t-s)$ elementos restantes para completar el $t-$subconjunto. De esta forma hay $\lambda_S \cdot \binom{k-s}{t-s}$ elementos en Y.

Por otro lado, el número de $t-$subconjuntos que contienen a S es $\binom{v-s}{t-s}$ y el número de bloques a los que pertenece T es, por definición, λ. Así, el número elementos en Y es $\lambda \cdot \binom{v-s}{t-s}$.

Igualando ambos resultados obtenemos $\lambda_S\binom{k-s}{t-s} = \lambda\binom{v-s}{t-s}$, y por tanto, es claro que λ_S es independiente del conjunto S y solo depende de su cardinal. De este modo se obtiene que $\lambda_s = \lambda\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$. □

En particular, un $t-(v,k,\lambda)$ diseño es un (v,k,r) diseño donde $r = \lambda_1 = \lambda\frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}$. Como consecuencia del resultado anterior se obtiene el siguiente corolario.

Corolario 2.4 *Todo $t-(v,k,\lambda)$ diseño es también un $s-(v,k,\lambda_s)$ diseño para todo $1 \leq s \leq t$.*

Ejemplo 12 *Dado el conjunto $X = \{1,2,3,4,5,6,7,8\}$ y el conjunto de bloques:*

$$\{1,2,3,5\},\ \{1,2,4,8\},\ \{1,2,6,7\},\ \{1,3,4,6\},\ \{1,3,7,8\},\ \{1,4,5,7\},\ \{1,5,6,8\},$$
$$\{2,3,4,7\},\ \{2,3,6,8\},\ \{2,4,5,6\},\ \{2,5,7,8\},\ \{3,4,5,8\},\ \{3,5,6,7\},\ \{4,6,7,8\},$$

observamos que todo subconjunto de tres elementos pertenece a un solo bloque, es decir, aparece una única vez. Luego el conjunto de elementos y bloques mencionados anteriormente forman un $3-(8,4,1)$ diseño.

Además, se puede apreciar que todo $2-$subconjunto pertenece al mismo número de bloques. Por ejemplo, el par $\{2,4\}$ aparece en los bloques $\{1,2,4,8\}$, $\{2,3,4,7\}$ y $\{2,4,5,6\}$ y el par $\{1,8\}$ pertenece a los bloques $\{1,2,4,8\}$, $\{1,3,7,8\}$ y $\{1,5,6,8\}$. Se observa rápidamente que esto ocurre para todo $2-$subconjunto de X, es decir, cada uno de ellos aparece exactamente en $\lambda_2 = 3$ bloques. De este modo el conjunto X y el conjunto de bloques anteriores forman un $2-(8,4,3)$ diseño.

Destacamos que también es un $1-(8,4,7)$ diseño, ya que todo elemento de X pertenece exactamente a $\lambda_1 = 7$ bloques.

Por último, es claro que no forman un $4-$diseño ya que por ejemplo, los subconjuntos $\{5,6,7,8\}$ y $\{2,3,4,5\}$ no pertenecen al diseño.

2.1. Diseños $S-$derivados y $S-$residuales

En general, no es tarea fácil construir $t-$diseños. Por este motivo, vamos a ver algunas formas de obtener otros $t-$diseños a partir de uno dado.

Definición 2.5 *Dado un $t-$diseño $D = (X,B)$ y un subconjunto S de X con $|S| = s \leq t$, llamamos diseño $S-$derivado de D respecto de S al que se obtiene eliminando los s elementos de S del conjunto X y está formado por todos los bloques de D que contienen a S eliminando de estos los s elementos. Denotaremos a este diseño por $D_S = (X_S, B_S)$.*

Dado un $t-$diseño, podemos obtener fácilmente los parámetros de un diseño $S-$derivado a partir del siguiente resultado.

Corolario 2.6 *El diseño $S-$derivado de un $t-(v,k,\lambda)$ diseño es también un diseño con parámetros $(t-s)-(v-s,k-s,\lambda)$ para todo $1 \leq s \leq t$.*

Demostración: Sea (X,B) un $t-(v,k,\lambda)$ diseño. Queremos ver que su diseño $S-$derivado (X_S, B_S) es un $(t-s)-$diseño con parámetros $(v-s,k-s,\lambda)$ para todo $1 \leq s \leq t$.

Por deficinión de diseño $S-$derivado, está claro que el número de elementos de este ha de ser $(v-s)$ y que el número de elementos que contiene cada bloque es $(k-s)$. Falta ver que todo $(t-s)-$ subconjunto pertenece al mismo número de bloques.
Sea Z un subconjunto de X_S con $(t-s)$ elementos. Entonces, el conjunto $Z \cup S \subseteq X$ tiene $|Z \cup S| = t-s+s = t$ elementos y por tanto está contenido en λ bloques B_i. De este modo, el conjunto Z estará en los bloques $B_{S_{i_1}}, ..., B_{S_{i_\lambda}}$, es decir, en λ bloques del conjunto B_S.

Así, acabamos de probar que todo $(t-s)-$ subconjunto pertenece al mismo número de bloques; λ, y por tanto, el diseño $s-$derivado de un $t-(v,k,\lambda)$ diseño es un $(t-s)-(v-s,k-s,\lambda)$ diseño para todo $1 \leq s \leq t$. □

En particular, si el conjunto S está formado por un solo elemento, se dice que el diseño D_S es una contracción de D respecto de S.

Si ahora en vez de tomar los bloques del diseño que contengan al subconjunto S (eliminando de estos los s elementos de dicho subconjunto) seleccionamos los bloques que no contengan a este, obtenemos un nuevo diseño. A este diseño se le denomina diseño $S-$residual. Para poder demostrar la existencia de este tipo de diseños, necesitamos el siguiente teorema.

Hemos visto en el teorema 2.3 que podemos conocer, dado un $s-$subconjunto, a cuántos bloques del diseño pertenece pero, ¿es posible conocer el número de bloques a los que pertenecen ciertos elementos con la condición de que no contengan a otros elementos fijados? Esta pregunta surgió, entre otros motivos, para dar origen a nuevos diseños a partir de uno dado, los cuales veremos a continuación. El siguiente teorema, que no es más que una generalización del teorema mencionado anteriormente, nos permitirá resolver esta cuestión.

Teorema 2.7 *Sea (X, B) un $t-(v, k, \lambda)$ diseño y los subconjuntos $S, Z \subseteq X$ tal que $|S| = s$, $|Z| = z$, $S \cap Z = \emptyset$ y $s + z \leq t$. Entonces, el número de bloques λ_s^z del $t-$diseño que contienen a todos los elementos de S y no contienen ningún elemento de Z es:*

$$\lambda_s^z = \lambda \frac{\binom{v-s-z}{k-s}}{\binom{v-t}{k-t}}.$$

Demostración: Consideremos primero el caso en el que $s = 0$, es decir, queremos ver cuántos bloques del diseño no contienen ningún elemento del subconjunto Z. Denotemos ese número por $\lambda_0^z(Z)$.
Si para cualquier elemento $x \in Z$ definimos el conjunto $B_x = \{B_i \in B : x \in B_i\}$, entonces para cualquier subconjunto $Z_0 \subseteq Z$ con $|Z_0| = h$, se tiene que

$$\left| \bigcap_{x \in Z_0} B_x \right| = \lambda_h.$$

Como se cumple que $h \leq z \leq t$, basta aplicar el teorema 2.3 al subconjunto Z_0 para obtener el resultado. Ahora, utilizando el principio de Inclusión-Exclusión, obtenemos la siguiente expresión:

$$|\{B_i \in B : B_i \cap Z = \emptyset\}| = \left| B \setminus \left(\bigcup_{x \in Z} B_x \right) \right| = \sum_{Z_0 \subseteq Z} (-1)^{|Z_0|} \left| \bigcap_{x \in Z_0} B_x \right|.$$

De esta forma

$$\lambda_0^z(Z) = \sum_{h=0}^{z} (-1)^h \binom{z}{h} \lambda_h,$$

y por tanto se tiene que el número $\lambda_0^z(Z)$ es independiente del subconjunto Z que tomemos, es decir, es una constante. Con el objetivo de simplificar dicha expresión, vamos a definir el siguiente conjunto y vamos a ver cúal es su cardinal. Sea el siguiente conjunto I:

$$I = \{(Z, B_i) : Z \subseteq X, |Z| = z, B_i \in B, Z \cap B_i = \emptyset\}.$$

Por un lado, existen $\binom{v}{z}$ formas de elegir el subconjunto Z y, para cada subconjunto Z, hay $\lambda_0^z(Z)$ bloques B_i tal que $Z \cap B_i = \emptyset$. Así, se tiene que $|I| = \binom{v}{z} \lambda_0^z(Z)$.

Por otro lado, existen b opciones de seleccionar un bloque B_i y, para cada uno de ellos, hay $\binom{v-k}{z}$

formas de elegir el subconjunto Z tal que $Z \cap B_i = \emptyset$. De este modo, $|I| = b\binom{v-k}{z}$.
Igualando ambas expresiones y utilizando el resultado del teorema 2.2 obtenemos que se cumple:

$$\lambda_0^z(Z) = \frac{b\binom{v-k}{z}}{\binom{v}{z}} = \lambda\frac{\binom{v-z}{k}}{\binom{v-t}{k-t}}.$$

Como queríamos probar.

Veamos ahora el caso en el que $s > 0$. Queremos conocer el número de bloques que contienen al subconjunto S pero no al subconjunto Z. Para ello basta considerar el diseño $S-$derivado del $t-$diseño inicial respecto del subconjunto S. De este modo, los bloques del diseño $S-$derivado serán aquellos bloques B_i del diseño inicial que contienen al subconjunto S eliminando de estos los elementos de dicho subconjunto. Una vez seleccionados esos bloques y aplicando el resultado anterior se obtienen aquellos que no contienen al subconjunto Z, que serán los mismos que hay en el diseño inicial y que contienen al subconjunto S pero no al subconjunto Z.
Sabemos por el corolario 2.6 que el diseño $S-$derivado de un $t-$diseño es un $(t-s)-(v-s,k-s,\lambda)$ diseño, luego aplicando el resultado anterior (caso $s = 0$) a estos diseños derivados obtenemos que se cumple

$$\lambda_s^z = \lambda\frac{\binom{v-s-z}{k-s}}{\binom{v-t}{k-t}}.$$

□

Definición 2.8 *Dado un $t-$diseño $D = (X, B)$ y un subconjunto S de X con $|S| = s \leq t$, llamamos diseño $S-$residual de D respecto de S al que se obtiene eliminando los elementos de dicho subconjunto de X y está formado por los bloques de D que no contienen ningún elemento de S. Denotaremos a este diseño por $D^S = (X^S, B^S)$.*

Corolario 2.9 *El diseño $S-$residual de un $t-(v,k,\lambda)$ diseño es también un diseño con parámetros $(t-s)-(v-s,k,\mu)$ para todo $1 \leq s \leq t$ donde*

$$\mu = \lambda\frac{\binom{v-t}{k-t+s}}{\binom{v-t}{k-t}}.$$

Demostración: Sea (X, B) un $t-(v,k,\lambda)$ diseño. Queremos probar que su diseño $S-$residual (X^S, B^S) es un $(t-s)-$diseño de parámetros $(v-s,k,\mu)$ para todo $1 \leq s \leq t$.

Como consecuencia directa de la definición de diseño $S-$residual sabemos que el número de elementos de dicho diseño es $(v-s)$, y que el número de elementos que contiene cada bloque sigue siendo k. Veamos entonces que todo $(t-s)-$subconjunto pertenece al mismo número de bloques.
Sea Z un subconjunto de X^S con $(t-s)$ elementos. Así, dicho conjunto Z pertenecerá a aquellos bloques B_i del diseño inicial que no contengan al conjunto S. Se cumple que $Z \cap S = \emptyset$ y $|Z| + |S| = (t-s) + s = t$. Por tanto, podemos aplicar el teorema 2.7 y obtenemos que dicho número de bloques es $\mu = \lambda_{(t-s)}^s = \lambda\frac{\binom{v-t}{k-t+s}}{\binom{v-t}{k-t}}$.

De este modo, acabamos de probar que todo $(t-s)-$subconjunto pertenece al mismo número de bloques; μ, y podemos concluir que el diseño $S-$residual de un $t-(v,k,\lambda)$ es un $(t-s)-(v-s,k,\mu)$ diseño para todo $1 \leq s \leq t$. □

Cabe destacar que, a diferencia de los diseños $S-$derivados, los diseños $S-$residuales tienen la misma uniformidad. Esto se debe a que los bloques de estos diseños son del mismo tamaño que los del $t-$diseño original.

Ejemplo 13 *Si tomamos el* $3-(8,4,1)$ *diseño del ejemplo 12 y seleccionamos, por ejemplo, el subconjunto* $S=\{5,6\}$*, podemos obtener dos diseños distintos formados por el mismo conjunto de elementos;* $X_S = X^S = \{1,2,3,4,7,8\}$.

Por un lado, si seleccionamos todos los bloques del diseño que contengan al subconjunto S *y eliminamos de estos los elementos de dicho subconjunto, obtenemos el conjunto de bloques formado por* $B_S = \{\{1,8\},\{2,4\},\{3,7\}\}$. *Este no es más que un* $\{5,6\}-$*diseño derivado del* $3-(8,4,1)$ *diseño, esto es, un diseño con parámetros* $1-(6,2,1)$.

Si ahora seleccionamos todos los bloques del diseño inicial que no contengan ningún elemento del subconjunto S*, obtenemos el diseño formado por el conjunto de bloques* $B^S = \{\{1,2,4,8\},\{1,3,7,8\},\{2,3,4,7\}\}$. *A este diseño se le denomina* $\{5,6\}-$*diseño residual del* $3-(8,4,1)$ *diseño, es decir, un diseño con parámetros* $1-(6,4,2)$.

Se observa rápidamente que podemos obtener numerosos diseños a partir de uno dado, basta con modificar los elementos del subconjunto S.

2.2. Sistemas de Steiner

Los sistemas de Steiner son un caso particular de los $t-$diseños y fue con estos, en particular con los sistemas triples de Steiner, con los que surgió el posterior estudio del resto de diseños. La particularidad de estos diseños se encuentra en que todo $t-$subconjunto ha de aparecer en un único bloque del diseño. Seguiremos las referencias [1], [7] y [9].

Definición 2.10 *Sea el diseño con parámetros* $t-(v,k,\lambda)$. *Llamamos sistema de Steiner a todo* $t-(v,k,\lambda)$ *diseño con* $\lambda = 1$.

Está claro que todo sistema de Steiner cumple las condiciones generales como $t-$diseño. En particular, de los resultados probados anteriormente, sabemos que el número de bloques de un sistema de Steiner de parámetros $t-(v,k,1)$ es $b = \binom{v}{t}/\binom{k}{t}$ y que, dado un $t-(v,k,1)$ diseño, también existe un $s-(v,k,\lambda_s)$ diseño con $\lambda_s = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$ para $1 \leq s \leq t$.

Teniendo en cuenta lo anterior, podemos garantizar que para todo $t-(v,k,1)$ diseño se cumple que $\binom{v-i}{t-i}/\binom{k-i}{t-i}$ es un número entero para todo $i = 0,1,...,t-1$. Este resultado nos va a proporcionar condiciones necesarias para la existencia de sistemas de Steiner. Por ejemplo, para $2-(v,k,1)$ diseños, $\binom{v}{2}/\binom{k}{2}$ y $\binom{v-1}{1}/\binom{k-1}{1}$ deben ser números enteros, esto es, $\frac{v(v-1)}{k(k-1)}$ y $\frac{v-1}{k-1}$ han de ser números enteros.

Además de cumplir todas las condiciones como t-diseño, todo sistema de Steiner satisface la siguiente propiedad:

Teorema 2.11 *En todo sistema de Steiner incompleto se cumple que:*

$$v \geq (t+1)(k-t+1).$$

Demostración: Sea (X,B) un sistema de Steiner con parámetros $t-(v,k,1)$. Por definición de sistema de Steiner, sabemos que dos bloques distintos tienen como máximo $t-1$ elementos en común, ya que cada $t-$subconjunto aparece en un solo bloque.
Supongamos que todo $(t+1)-$subconjunto de X está en al menos un bloque. De este modo, el diseño original es también un $(t+1)-(v,k,\alpha)$ diseño con $\alpha \geq 1$. Aplicando el teorema 2.3 tenemos que

$\lambda = 1 = \alpha\frac{\binom{v-t}{t+1-t}}{\binom{k-t}{t+1-t}} = \alpha\frac{v-t}{k-t}$, que es absurdo, ya que $v > k$ por ser un diseño incompleto y $\alpha \geq 1$. Por lo tanto, existe al menos un $(t+1)-$subconjunto que no está contenido en ningún bloque del diseño inicial. Llamemos Y a dicho $(t+1)-$subconjunto.

Para cada uno de los $t+1$ subconjuntos $T \subseteq Y$ con $|T| = t$ existe un único bloque B_T del diseño que lo contiene, y cada uno de esos bloques B_T contiene a su vez a $k-t$ elementos que no pertenecen a Y.

Por otro lado, cada elemento que no está en Y aparece como máximo en uno de los bloques B_T, ya que dos de estos bloques tienen $t-1$ elementos de Y en común. Supongamos lo contrario.
Sean $T_1, T_2, ..., T_{t+1}$ los $t+1$ subconjuntos de Y con t elementos cada uno. Claramente se tiene que $|T_i| \cap |T_j| = t-1$, con T_i contenido en el bloque B_i y T_j contenido en el bloque B_j. Si tomamos un elemento $y \notin Y$ que pertenezca a ambos bloques, tendríamos que $B_i \cap B_j = (T_i \cap T_j) \cup \{y\}$ y por tanto $|B_i \cap B_j| = t$, que es absurdo por definición de sistema de Steiner.
Con esto, la unión de todos los bloques B_T del diseño se puede escribir como

$$v \geq |\cup B_T| = |X| + \sum_{T \subset X} |B_T \setminus X| = (t+1) + (t+1)(k-t),$$

es decir, contiene a $(t+1)(k-t+1)$ elementos.
En consecuencia, queda probado que $v \geq (t+1)(k-t+1)$ en todo sistema de Steiner. □

Dentro de este tipo de diseños cabe destacar la existencia de los $t-$diseños en el caso especial en el que los parámetros satisfacen $k = t+1$. Este problema fue planteado por Steiner (1853) quien, aparentemente sin conocer el trabajo de Kirkman sobre los sistemas triples de Steiner, generalizó el resultado. El caso $t = 2$ se corresponde con los denominados sistemas triples de Steiner y el caso $t = 3$ con los denominados sistemas cuádruples de Steiner, los cuales veremos a continuación.

Los sistemas triples de Steiner son un caso particular de los sistemas de Steiner tomando $t = 2$, es decir, un sistema triple de Steiner es un $2-(v, 3, 1)$ diseño.

Aplicando el teorema 2.2 y el teorema 2.3, sabemos que el número de bloques de un $2-(v, 3, 1)$ diseño es $\frac{v(v-1)}{6}$ y que cada elemento aparece en $\frac{v-1}{2}$ bloques.

El siguiente teorema da una condición necesaria que satisface todo sistema triple de Steiner. Más adelante, construyendo los sistemas triples de Steiner correspondientes, veremos que esta condición es también suficiente.

Teorema 2.12 *Si existe un sistema triple de Steiner, entonces* $v \equiv 1$ *o* $3 \pmod 6$.

Demostración: Sea $2-(v, 3, 1)$ un sistema triple de Steiner. Sabemos que para todo $t-(v, k, 1)$ diseño, se cumple que $\binom{v-i}{t-i}/\binom{k-i}{t-i}$ es un número entero para todo $i = 0, 1, ..., t-1$. Por ello, en este caso $\binom{v}{2}/\binom{3}{2}$ y $\binom{v-1}{1}/\binom{2}{1}$ han de ser números enteros. Es decir, $v(v-1) \equiv 0 \pmod 6$ y $v-1 \equiv 0 \pmod 2$. Por lo tanto $v \equiv 1$ o $3 \pmod 6$. □

Además, existe cierta relación entre la existencia de sistemas triples de Steiner para determinados parámetros. En concreto, se tiene el siguiente resultado (ver [1]):

Teorema 2.13 *Si existe un sistema triple de Steiner con* n *elementos, entonces también existe un sistema triple de Steiner con* $2n+1$ *elementos.*

Por otro lado, los sistemas cuádruples de Steiner no son más que sistemas de Steiner con $t = 3$, es decir, un sistema cuádruple de Steiner es un $3-(v, 4, 1)$ diseño.

Del mismo modo, aplicando los teoremas 2.2 y 2.3 obtenemos que el número de bloques de un $3-(v, 4, 1)$ diseño es $\frac{v(v-1)(v-2)}{24}$ y que cada elemento aparece en $\frac{(v-1)(v-2)}{6}$ bloques.

Una condición necesaria que satisface todo sistema cuádruple de Steiner es la siguiente:

Teorema 2.14 *Si existe un sistema cuádruple de Steiner, entonces* $v \equiv 2$ *o* $4 \pmod 6$.

Demostración: La demostración es inmediata, tal y como ocurría en la demostración para sistemas triples de Steiner. Sea $3-(v, 4, 1)$ un sistema cuádruple de Steiner. Sabemos que para todo $t-(v, k, 1)$ diseño, se cumple que $\binom{v-i}{t-i}/\binom{k-i}{t-i}$ es un número entero para todo $i = 0, 1, ..., t-1$. Por ello, en este caso $\binom{v}{3}/\binom{4}{3}$, $\binom{v-1}{2}/\binom{3}{2}$ y $\binom{v-2}{1}/\binom{2}{1}$ han de ser números enteros. Es decir, $v(v-1)(v-2) \equiv 0 \pmod{24}$, $(v-1)(v-2) \equiv 0 \pmod 6$ y $(v-2) \equiv 0 \pmod 2$. Por lo tanto $v \equiv 2$ o $4 \pmod 6$. □

De nuevo, para los sistemas cuádruples de Steiner, conocemos algunas relaciones de existencia de estos diseños para ciertos parámetros, como muestra el siguiente resultado (ver referencia [1]):

Teorema 2.15 *Se tiene que:*

1. *Existe un sistema cuádruple de Steiner con* 2^n *elementos para todo* $n \geq 2$.
2. *Si existe un sistema cuádruple de Steiner con* n *elementos, entonces también existe un sistema cuádruple de Steiner con* $2n$ *elementos.*

Solo hemos mencionado la existencia de sistemas de Steiner para $t = 2, 3$ ya que, hasta ahora, no se conocen muchos sistemas de Steiner para $t > 3$. En particular, se conocen algunos $5-(v, k, 1)$ diseños de parámetros, por ejemplo, $5-(12, 6, 1)$, $5-(24, 8, 1)$ o $5-(132, 6, 1)$ entre otros (ver [1]). Cabe destacar que todavía no se ha descubierto ningún sistema de Steiner para $t > 5$.

2.3. 2-diseños

Acabamos de ver un caso particular de $t-$diseños, aquellos en los que $\lambda = 1$. Ahora, vamos a estudiar los diseños en los que $t = 2$, es decir, los $2-$diseños, conocidos como diseños balanceados. Este tipo de diseños son los más estudiados en la teoría del diseño.

Supongamos a partir de ahora que todos los $2-$diseños con los que vamos a trabajar son incompletos, es decir, que no contengan ningún bloque formado por el conjunto total de elementos del diseño.
Un caso particular del teorema 2.3 muestra el número de bloques a los que pertenece cada elemento en este tipo de diseños.

Corolario 2.16 *Sea un* $2-(v, k, \lambda)$ *diseño con* b *bloques. Entonces cada elemento aparece exactamente en* $r = \lambda\frac{(v-1)}{(k-1)}$ *bloques.*

En el capítulo 1 vimos la noción de diseño complementario. Este diseño se obtenía a partir de uno dado, modificando los bloques B_i por sus complementarios. En el caso de un $2-$diseño, su diseño complementario es también un $2-$diseño.

Proposición 2.17 *El diseño complementario de un* $2-(v,k,\lambda)$ *diseño es también un* $2-$*diseño con parámetros* $2-(v,v-k,b-2r+\lambda)$.

Demostración: Sea (X,B) un $2-$diseño con parámetros $2-(v,k,\lambda)$. A partir de la definición de diseño complementario es claro que $\bar{D}$ cumple $|\bar{X}|=v$ y cada bloque $|\bar{B}_i|=v-k$. Basta probar entonces que todo $2-$subconjunto se encuentra en el mismo número de bloques.
Un par de elementos $\{x,y\}$ de X con $x\neq y$ estará contenido en algún bloque $\bar{B}_i$ si el bloque B_i no contiene ni al elemento x ni a y.
Por definición de $2-$diseño sabemos que el número de bloques a los que pertenece la pareja $\{x,y\}$ es λ y que el número de bloques que contienen a cada elemento de X es r. De este modo, el número de bloques que contienen al elemento x pero no al y ó que contienen al elemento y pero no al x será $(r-\lambda)$. Así, el número de bloques $\bar{B}_i$ que contienen a $\{x,y\}$ es:

$$\bar{\lambda}=b-2(r-\lambda)-\lambda=b-2r+\lambda.$$

Esto prueba que el diseño complementario de un $2-(v,k,\lambda)$ diseño es también un $2-$diseño con parámetros $2-(v,v-k,b-2r+\lambda)$. □

A priori, no podemos decir lo mismo para el diseño dual de un $2-$diseño. Más adelante veremos que el diseño dual de un $2-$diseño será un $2-$diseño si este satisface ciertas propiedades de simetría.

Nos centramos ahora en estudiar una condición necesaria muy importante para la existencia de $2-$diseños, que afirma que todo $2-$diseño debe tener, al menos, tantos bloques como elementos. A esta condición se la denomina *Desigualdad de Fisher* (1940) [14] y se obtiene teniendo en cuenta la siguiente proposición, que da la expresión que cumple toda matriz de incidencia de estos diseños.

Proposición 2.18 *Sea* A *la matriz de incidencia de un* $2-(v,k,\lambda)$ *diseño,* $J_{v\times v}$ *la matriz con todos los elementos igual a uno e* $I_{v\times v}$ *matriz identidad. Entonces*

$$AA^T=(r-\lambda)I_v+\lambda J_v.$$

Demostración: Sea A la matriz de incidencia de un $2-(v,k,\lambda)$ diseño. El elemento a_{ij} será uno sí, y solo sí, el elemento i pertenece al bloque j, o cero en caso contrario.
Si consideramos el producto $AA^T=(a'_{ij})$, cada elemento a'_{ij} será el producto de la $i-$ésima fila de A por la $j-$ésima columna de A^T o lo que es lo mismo, el producto de la $i-$ésima fila por la $j-$ésima fila de A. Entonces, podemos escribir cada elemento a'_{ij} de la forma

$$a'_{ij}=\sum_{n=1}^{b}a_{in}a_{jn} \tag{2.1}$$

Así, cada producto $a_{in}a_{jn}$ será uno si ambos elementos i,j pertenecen al mismo bloque B_n. Distingamos dos casos:

- Si $i=j$ se cumple que:

$$a'_{ii}=\sum_{n=1}^{b}a_{in}a_{in}=\sum_{n=1}^{b}a_{in}^2 \tag{2.2}$$

  la suma es el número de bloques a los que pertenece el elemento i, luego $a'_{ii}=r$.

- Si $i\neq j$, la suma corresponde al número de bloques que contienen a los elementos i,j a la vez, es decir, $a'_{ij}=\lambda$.

Por lo tanto,

$$AA^T = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & & \ddots & \vdots \\ \lambda & \cdots & \lambda & r \end{pmatrix}_{v\times v} \tag{2.3}$$

Que es lo mismo que $AA^T = rI_v + \lambda(J_v - I_v)$, es decir, $AA^T = (r-\lambda)I_v + \lambda J_v$. □

Teorema 2.19 ***(Desigualdad de Fisher)*** *En todo $2-(v,k,\lambda)$ diseño con b bloques, se cumple que $b \geq v$.*

Demostración: Consideremos la matriz AA^T de la proposición 2.18 que es de la forma:

$$AA^T = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & & \ddots & \vdots \\ \lambda & \cdots & \lambda & r \end{pmatrix}_{v\times v} \tag{2.4}$$

Queremos probar que se cumple $b \geq v$. Para ello, primero vamos a ver que la matriz AA^T es no singular calculando su determinante.

Dada la matriz AA^T, si restamos la primera fila al resto de filas obtenemos:

$$|AA^T| = \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda - r & r-\lambda & 0 & & 0 \\ \lambda - r & 0 & r-\lambda & & 0 \\ \vdots & & & \ddots & \vdots \\ \lambda - r & 0 & 0 & \cdots & r-\lambda \end{vmatrix} \tag{2.5}$$

Y si ahora sumamos a la primera columna la suma del resto de columnas:

$$|AA^T| = \begin{vmatrix} r+(v-1)\lambda & \lambda & \lambda & \cdots & \lambda \\ 0 & r-\lambda & 0 & & 0 \\ 0 & 0 & r-\lambda & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & r-\lambda \end{vmatrix} \tag{2.6}$$

De esta forma obtenemos que $|AA^T| = (r+(v-1)\lambda)(r-\lambda)^{v-1}$.
Aplicando el corolario 2.16 sabemos que se cumple que $r(k-1) = \lambda(v-1)$, luego podemos escribir

$$|AA^T| = (r+(k-1)r)(r-\lambda)^{v-1} = rk(r-\lambda)^{v-1}.$$

Y esta expresión es distinta de cero ya que, de nuevo por el corolario 2.16, sabemos que $r = \lambda\frac{(v-1)}{(k-1)}$, y como $k < v$ por ser un diseño incompleto, siempre se cumple que $r > \lambda$. Por lo tanto, el determinante $|AA^T|$ es distinto de cero y con ello, el $rango(AA^T) = v$.

Finalmente, teniendo en cuenta que $rango(AA^T) \leq rango(A)$ y que la matriz A de tamaño $v \times b$ tiene $rango(A) \leq b$, obtenemos el resultado $v = rango(AA^T) \leq rango(A) \leq b$. □

En el caso en el que se cumpla la igualdad, es decir, si en un diseño hay el mismo número de elementos

que de bloques, obtenemos los $2-(v,k,\lambda)$ diseños que se conocen como diseños simétricos. En estos, de la ecuación $bk = vr$, se deduce que $k = r$.

En particular, este teorema se puede generalizar a $2s-$diseños y $(2s+1)-$diseños con los siguientes resultados de D.K. Ray-Chaudhuri y R.M. Wilson [20] (1975), conocidos como las *Generalizaciones de la Desigualdad de Fisher*.

Teorema 2.20 *Se tiene que:*

I) *En todo* $2s-(v,k,\lambda)$ *diseño con* $v \geq k+s$ *se cumple que* $b \geq \binom{v}{s}$.

II) *En todo* $(2s+1)-(v,k,\lambda)$ *diseño con* $v \geq k+s+1$ *se cumple que* $b \geq 2\binom{v-1}{s}$.

2.3.1. Diseños simétricos

Definición 2.21 *Sea* $2-(v,k,\lambda)$ *un diseño. Se dice que es un diseño simétrico si se cumple* $v = b$.

Por el teorema 1.3, la condición $v = b$ es equivalente a que $k = r$, y con ello, aplicando el corolario 2.16 también es equivalente a que se cumpla $\lambda(v-1) = k(k-1)$. Por tanto, es una condición necesaria pero no suficiente en sí misma para garantizar la existencia de un diseño simétrico.

En este tipo de diseños introduciremos el concepto de orden del diseño. Diremos que el orden de un diseño simétrico con parámetros $2-(v,k,\lambda)$ es n, donde $n = k-\lambda$.

En particular, si $n = 1$, el diseño simétrico será el trivial. Esto se debe a que $1 = k-\lambda$ sí, y solo sí, $k = v-1$ (basta tener en cuenta que se cumple $\lambda(v-1) = k(k-1)$). Como $v = b$, el diseño estará formado por todos los posibles $(v-1)-$subconjuntos de X y por lo tanto, $\lambda = k\frac{k-1}{v-1} = k-1 = v-2$. De esta forma, el diseño simétrico trivial tiene como parámetros $2-(v, v-1, v-2)$.

Por lo tanto, para todo diseño simétrico distinto del trivial, se tiene que $k < v-1$. Supongamos a partir de ahora que todo diseño simétrico con el que trabajemos es distinto del trivial.

Cabe destacar que la matriz de incidencia de un diseño simétrico no tiene por qué ser simétrica, como se puede ver en el siguiente ejemplo.

Ejemplo 14 *Sea el diseño* D *de parámetros* $2-(15,7,3)$ *formado por el conjunto de elementos* $X = \{1,2,3,...,14,15\}$ *y el conjunto de bloques:*

$\{1,2,3,4,5,6,7\}$,	$\{1,6,7,8,9,14,15\}$,	$\{2,5,7,9,10,13,14\}$,
$\{1,2,3,8,9,10,11\}$,	$\{1,6,7,10,11,12,13\}$,	$\{3,4,6,9,11,13,14\}$,
$\{1,2,3,12,13,14,15\}$,	$\{2,4,6,8,10,12,14\}$,	$\{3,4,7,9,10,12,15\}$,
$\{1,4,5,8,9,12,13\}$,	$\{2,4,7,8,11,13,15\}$,	$\{3,5,6,8,10,13,15\}$,
$\{1,4,5,10,11,14,15\}$,	$\{2,5,6,9,11,12,15\}$,	$\{3,5,7,8,11,12,14\}$.

Se puede observar a simple vista que es un diseño simétrico cuyo orden es $n = 4$. *Por ser un diseño simétrico, su matriz* A *de incidencia es cuadrada, pero se puede comprobar que no es simétrica.*

Ya conocemos las condiciones que satisfacen los parámetros de todo diseño simétrico. El siguiente teorema nos permite saber, además, el número de elementos que tienen en común dos bloques distintos del diseño. Este resultado nos va a ser de gran utilidad para probar el resto de la sección.

Teorema 2.22 *En un diseño simétrico, la intersección de dos bloques cualesquiera es* λ.

Demostración: Sea $2-(v,k,\lambda)$ un diseño simétrico y sea A su matriz de incidencia. En la proposición 2.18 probamos que $AA^T = (r-\lambda)I_v + \lambda J_v$ y además, de la demostración del teorema 2.19, sabemos que su determinante $|AA^T| = rk(r-\lambda)^{v-1}$ es distinto de cero.
Ahora, por ser un diseño simétrico, la matriz A es cuadrada, es decir, $|A| = |A^T|$, y por tanto el determinante de A es no nulo. Si multiplicamos por A a la derecha de la expresión $AA^T = (r-\lambda)I_v+\lambda J_v$ obtenemos:

$$AA^TA = ((r-\lambda)I_v + \lambda J_v)A = A((r-\lambda)I_v + \lambda J_v) = AAA^T, \tag{2.7}$$

ya que $J_vA = AJ_v$, y multiplicando a la izquierda por A^{-1} obtenemos que $AA^T = A^TA$.
Sabemos que la entrada $(i,j)-$ésima de la matriz AA^T es el producto de la fila i de la matriz A por la columna j de la matriz A^T, esto es, con la fila j de la matriz A. Dicho producto es el número de bloques al que pertenece el par de elementos $\{x_i, x_j\}$, es decir, λ si $i \neq j$.
Sin embargo, la entrada $(i,j)-$ésima de la matriz A^TA es el producto de la fila i de A^T, es decir, de la columna i de la matriz A, con la columna j de la matriz A. Y este producto no es más que el número de elementos que tienen en común los bloques B_i y B_j si $i \neq j$.
De la ecuación (2.7), como ambas matrices son iguales, podemos concluir que $|B_i \cap B_j| = \lambda$ para $i \neq j$. □

El siguiente corolario es consecuencia directa de la proposición 2.17 aplicada a 2-diseños simétricos.

Corolario 2.23 *El diseño complementario de un $2-(v,k,\lambda)$ diseño simétrico es un diseño simétrico con parámetros $2-(v,v-k,\bar{\lambda})$, con $\bar{\lambda} = v-2k+\lambda > 0$.*

El orden del diseño complementario de un diseño simétrico es también $\bar{n} = \bar{k}-\bar{\lambda} = (v-k)-(v-2k+\lambda) = k-\lambda = n$. Además, $\bar{\lambda} = v-2k+\lambda > 0$ ya que suponemos que el diseño simétrico es distinto del trivial y por ello $k < v-1$, es decir, $\lambda < k-1$. Con esto, de la igualdad $\lambda(v-k) = \lambda(v-1)+\lambda(1-k) = k(k-1)-\lambda(k-1) = (k-1)(k-\lambda)$ se tiene que $v-k > k-\lambda$, esto es, $v-2k+\lambda > 0$.

El diseño complementario de un diseño simétrico sigue siendo un diseño simétrico. Veamos ahora que el diseño dual de un diseño simétrico es también un diseño simétrico.

Teorema 2.24 *El diseño dual de un $2-(v,k,\lambda)$ diseño es un $2-$diseño sí, y solo sí, el diseño inicial es simétrico.*

Demostración: Comencemos viendo que la condición de simétrico es necesaria. Sea $2-(v,k,\lambda)$ un diseño D de forma que su diseño dual D^T es un $2-$diseño. Supongamos que D no es simétrico. Entonces se tiene que $b > v$, y por tanto, como $b^T = v$ y $v^T = b$, se tendría que $v^T \geq b^T$. Y esto es absurdo ya que suponíamos que el diseño dual de D era un $2-$diseño.

Veamos ahora que es suficiente. Sea $2-(v,k,\lambda)$ un diseño simétrico. Sabemos que el diseño dual de este diseño tiene como parámetros $v^T = b$ y $k^T = r$, y por ser simétrico se tiene que $v^T = v$ y que $k^T = k$. Basta probar entonces que todo $2-$subconjunto está en el mismo número de bloques. Dados x e y dos elementos distintos de D^T, queremos ver que ambos pertenecen a un número fijo de bloques de D^T, es decir, queremos ver cúantos elementos de D tienen en común dos bloques de D. Por ser D un $2-$diseño dicho número es λ, ya que es el número de elementos que contiene la intersección de dos bloques cualesquiera de D. Por tanto, el diseño dual de un diseño simétrico es un $2-$diseño. □

Además, es fácil ver que el diseño dual de un diseño simétrico es también simétrico.

Los resultados vistos anteriormente nos permiten obtener diseños simétricos a partir de otros diseños simétricos. Existen más formas de obtener nuevos $2-$diseños a partir de diseños simétricos. En esta sección presentaremos los más conocidos y estudiados; los diseños derivados y los diseños residuales de los diseños simétricos.

Definición 2.25 *Dado un diseño simétrico $D = (X, B)$, llamamos diseño derivado de D respecto de un bloque $B_i \in B$ al que se obtiene de tomar como conjunto de elementos los del propio bloque B_i y como conjunto de bloques los que se obtienen al intersecar el bloque B_i con el resto de bloques de B. Denotamos a este diseño por $D_{\{B_i\}} = (X_{\{B_i\}}, B_{\{B_i\}})$.*

Proposición 2.26 *El diseño derivado de un $2-(v, k, \lambda)$ diseño simétrico es un $2-$diseño de parámetros $2 - (k, \lambda, \lambda - 1)$ con $\lambda \geq 2$.*

Demostración: Sea un (X, B) un diseño simétrico con parámetros $2 - (v, k, \lambda)$. Queremos ver que el diseño derivado $(X_{\{B_i\}}, B_{\{B_i\}})$ de D respecto de un bloque B_i , es un $2-$diseño.

Por definición de diseño derivado, el número de elementos de $X_{\{B_i\}}$ será el número de elementos que tenga el bloque B_i de B, es decir, k.

Por otro lado, el número de elementos de cada bloque $B_{\{B_i\}_j}$ de $B_{\{B_i\}}$ será la intersección del bloque B_i con el bloque B_j, y del teorema 2.22 sabemos que dicho número es λ. Para que exista un diseño con esos parámetros se tiene que cumplir que $\lambda < k$. Y esto es fácil de comprobar ya que como D es un diseño simétrico con $v > k$ y tal que $\lambda(v - 1) = k(k - 1)$, λ ha de ser estrictamente menor que k.

Finalmente, vamos a ver que todo $2-$subconjunto de $X_{\{B_i\}}$ pertenece al mismo número de bloques. Sea el subconjunto $T \subseteq B_i$ formado por dos elementos y que pertenece, por definición, a λ bloques de D con $\lambda \geq 2$. Así, como en el diseño $D_{\{B_i\}}$ el bloque B_i es el propio conjunto de elementos, el subconjunto T pertenecerá a $\lambda - 1$ bloques.

Podemos concluir que el diseño derivado de D respecto de un bloque B_i de B es un $2-$diseño de parámetros $2 - (k, \lambda, \lambda - 1)$ con $\lambda \geq 2$. □

Definición 2.27 *Dado un diseño simétrico $D = (X, B)$, se define diseño residual de D respecto de un bloque $B_i \in B$ al diseño que tiene como conjunto de elementos a $X \setminus B_i$ y como conjunto de bloques al que se obtiene de eliminar los elementos de B_i del resto de bloques de B. Denotamos a este diseño por $D^{\{B_i\}} = (X^{\{B_i\}}, B^{\{B_i\}})$.*

Proposición 2.28 *El diseño residual de un $2-(v, k, \lambda)$ diseño simétrico es un $2-$diseño de parámetros $2 - (v - k, k - \lambda, \lambda)$ con $k \geq \lambda + 2$.*

Demostración: Sea un (X, B) un diseño simétrico con parámetros $2 - (v, k, \lambda)$. Queremos probar que el diseño residual $(X^{\{B_i\}}, B^{\{B_i\}})$ de D respecto de un bloque B_i de B es un $2-$diseño.

Claramente, el número de elementos del conjunto $X^{\{B_i\}}$ es $v - k$, ya que por definición de diseño derivado, eliminamos de X todos los elementos que pertenecen al bloque B_i.

Por otro lado, como el conjunto de bloques $B^{\{B_i\}}$ está formado por todos los bloques de B eliminando de estos los elementos del bloque B_i, podemos definir los bloques de $B^{\{B_i\}_j}$ como $B^{\{B_i\}_j} = B^{\{B_i\}_j} \setminus (B^{\{B_i\}_j} \cap B_i)$. Así, aplicando el teorema 2.22 podemos concluir que el número de elementos que contiene cada bloque de $B^{\{B_i\}}$ es $k - \lambda$.
Para que exista un diseño con estos parámetros, se tiene que cumplir que $v - k > k - \lambda$, es decir, que $v > 2k - \lambda$. Supongamos que se cumple lo contrario. Por ser un $2 - (v, k, \lambda)$ diseño simétrico se cumple que $k(k - 1) = \lambda(v - 1)$, esto es, $k(k - 1) = \lambda(v - 1) \leq \lambda(2k - \lambda - 1)$. Operando dicha expresión obtenemos que $(k - \lambda)(k - \lambda - 1) \leq 0$, pero por hipótesis $k \geq \lambda + 2$, y por tanto dicha desigualdad no se cumple, llegando a un absurdo. De este modo tenemos que $v - k > k - \lambda$.

Por último, hemos de probar que todo $2-$subconjunto de $X^{\{B_i\}}$ pertenece al mismo número de bloques.

Dado el subconjunto $T \subseteq X^{\{B_i\}}$, sabemos que pertenece a λ bloques de D y, como T no pertenece al bloque B_i, tampoco pertenecerá a la intersección de B_i con el resto de bloques de B, es decir, estará en los mismos bloques a los que pertenecía en el diseño inicial. De esta forma, todo $2-$subconjunto estará en λ bloques de $D^{\{B_i\}}$.

Podemos concluir que el diseño residual de D respecto de un bloque B_i de B es un $2-$diseño de parámetros $2-(v-k, k-\lambda, \lambda)$ con $k \geq \lambda + 2$. □

Ejemplo 15 *Consideremos el diseño simétrico D del ejemplo 14 con parámetros $2-(15,7,3)$ y tomemos el bloque $B_i = \{1,4,5,10,11,14,15\}$.*
El diseño derivado de D respecto del bloque B_i tiene como conjunto de elementos $X_{\{B_i\}}$ los del propio bloque y como conjunto de bloques $B_{\{B_i\}}$:

$$\begin{array}{ccccccc} \{1,4,5\}, & \{1,10,11\}, & \{1,14,15\}, & \{4,10,14\}, & \{4,11,14\}, & \{5,10,14\}, & \{5,10,15\}, \\ \{1,4,5\}, & \{1,10,11\}, & \{1,14,15\}, & \{4,10,15\}, & \{4,11,15\}, & \{5,11,14\}, & \{5,11,15\}. \end{array}$$

Claramente el diseño derivado $D_{\{B_i\}} = (X_{\{B_i\}}, B_{\{B_i\}})$ es un $2-$diseño con parámetros $2-(7,3,2)$.

Por otro lado, el diseño residual de D respecto del bloque B_i tiene como conjunto de elementos a $X^{\{B_i\}} = \{2,3,6,7,8,9,12,13\}$ y como conjunto de bloques $B^{\{B_i\}}$:

$$\begin{array}{ccccccc} \{2,3,6,7\}, & \{2,3,12,13\}, & \{2,6,9,12\}, & \{2,7,9,13\}, & \{3,6,9,13\}, & \{3,7,9,12\}, & \{6,7,12,13\}, \\ \{2,3,8,9\}, & \{2,6,8,12\}, & \{2,7,8,13\}, & \{3,6,8,13\}, & \{3,7,8,12\}, & \{6,7,8,9\}, & \{8,9,12,13\}. \end{array}$$

El diseño residual $D^{\{B_i\}} = (X^{\{B_i\}}, B^{\{B_i\}})$ es por tanto un $2-$diseño con parámetros $2-(8,4,3)$.

Una vez hemos explicado las propiedades que cumplen los diseños simétricos y presentado diversas formas de obtener nuevos diseños a partir de estos, vamos a probar una condición necesaria para la existencia de $2-$diseños simétricos.

Teorema 2.29 *Supongamos que existe un $2-(v,k,\lambda)$ diseño simétrico de orden $n = k - \lambda$, entonces*

$$4n - 1 \leq v \leq n^2 + n + 1. \tag{2.8}$$

Demostración: Sea $2-(v,k,\lambda)$ un diseño simétrico de orden $n = k - \lambda$. Por el corolario 2.23 sabemos que su diseño complementario es también un diseño con $\bar{\lambda} = v - 2k + \lambda > 0$.
Operando los parámetros de ambos diseños obtenemos que $\lambda + \bar{\lambda} = v - 2k + 2\lambda = v - 2n$ y

$$\lambda\bar{\lambda} = \lambda(v - 2k + \lambda) = \lambda v - 2k\lambda + \lambda^2 = \lambda(v-1) + \lambda - 2k\lambda + \lambda^2 = k(k-1) + \lambda - 2k\lambda + \lambda^2 =$$
$$= k^2 + \lambda^2 - 2k\lambda - k + \lambda = (k-\lambda)^2 - (k-\lambda) = n^2 - n = n(n-1).$$

Sabemos que para todo x e y números reales se cumple $(x+y)^2 \geq 4xy$. En particular, si tomamos $x = \lambda$ e $y = \bar{\lambda}$ tenemos que $(\lambda + \bar{\lambda})^2 \geq 4\lambda\bar{\lambda}$, es decir, $(v-2n)^2 \geq 4n(n-1)$.
Sin embargo, el valor $4n(n-1)$ no es un cuadrado perfecto, por lo que ha de ser $(v-2n)^2 > 4n(n-1)$, y así $(v-2n)^2 \geq 4n^2 - 4n + 1 = (2n-1)^2$.
Como $\lambda + \bar{\lambda} = v - 2n > 0$, obtenemos $v - 2n \geq 2n - 1$, esto es, $v \geq 4n - 1$.
Para la otra desigualdad vamos a operar de nuevo con λ y $\bar{\lambda}$. Sabemos que $\lambda, \bar{\lambda} \geq 1$, luego

$$0 \leq (\lambda - 1)(\bar{\lambda} - 1) = \lambda\bar{\lambda} - (\lambda + \bar{\lambda}) + 1 = n(n-1) - (v - 2n) + 1,$$

es decir, $v \leq n^2 + n + 1$. □

Esta es, por tanto, una condición necesaria pero no suficiente para la existencia de $2-$diseños simétricos. Ahora, vamos a ver que si v toma los valores extremos de la desigualdad, obtenemos nuevos diseños simétricos.

Teorema 2.30 *Si existe un diseño simétrico D con $v = n^2 + n + 1$ y orden $n = k - \lambda$, entonces el diseño D o su complementario $\bar{D}$ es un $2 - (n^2 + n + 1, n + 1, 1)$ diseño simétrico.*

Demostración: Supongamos que existe un diseño simétrico D con parámetros $2 - (v, k, \lambda)$ tal que $v = n^2 + n + 1$. En la demostración del teorema 2.29 vimos que si $v = n^2 + n + 1$ entonces $\lambda = 1$ ó $\bar{\lambda} = 1$. Queremos ver que en ambos casos existe un diseño con parámetros $2 - (n^2 + n + 1, n + 1, 1)$, es decir, basta ver que $k = n + 1$ en ambos casos.

Si $\lambda = 1$, entonces $n = k - 1$, es decir, $k = n + 1$. Y de esta forma obtenemos que D es un $2 - (n^2 + n + 1, n + 1, 1)$ diseño simétrico.

De la misma forma, si $\bar{\lambda} = 1$, entonces $\bar{n} = \bar{k} - 1$, es decir, $\bar{k} = \bar{n} + 1 = n + 1$. Por lo tanto, el diseño complementario $\bar{D}$ de D es un $2 - (n^2 + n + 1, n + 1, 1)$ diseño simétrico. □

Teorema 2.31 *Si existe un diseño simétrico D con $v = 4n - 1$ y orden $n = k - \lambda$, entonces el diseño D o su complementario $\bar{D}$ es un $2 - (4n - 1, 2n - 1, n - 1)$ diseño simétrico.*

Demostración: Supongamos que existe un diseño simétrico D con parámetros $2 - (v, k, \lambda)$ tal que $v = 4n - 1$.
Sabemos que si un polinomio de segundo grado con coeficientes a, b y c tal que $ax^2 + bx + c$ tiene como raíces r_1 y r_2, entonces $b = -a(r_1 + r_2)$ y $c = ar_1r_2$.
En particular, si tomamos $r_1 = \lambda$ y $r_2 = \bar{\lambda}$, tenemos que $\lambda + \bar{\lambda} = v - 2n = 2n - 1$ y $\lambda\bar{\lambda} = n(n - 1)$ (visto en la demostración del teorema 2.29). Por lo tanto, el polinomio $x^2 - (2n-1)x + n(n-1)$ tendrá como raíces a n y a $(n - 1)$.

Supongamos que $\lambda = n - 1$. Entonces $n = k - \lambda = k - n + 1$, es decir, $k = 2n - 1$. Así tenemos que D es un diseño simétrico con parámetros $2 - (4n - 1, 2n - 1, n - 1)$.

Ahora supongamos que $\bar{\lambda} = n - 1$. Entonces $\bar{n} = \bar{k} - \bar{\lambda} = \bar{k} - \bar{n} + 1 = \bar{k} - n + 1$, es decir, $\bar{k} = 2n - 1$. Así, el diseño complementario $\bar{D}$ de D es un diseño simétrico de parámetros $2 - (4n - 1, 2n - 1, n - 1)$.
□

Un diseño con parámetros $2-(4n-1, 2n-1, n-1)$ se conoce como diseño de Hadamard de orden n ya que la existencia de estos diseños está estrechamente relacionada con la de determinadas matrices, llamadas matrices de Hadamard. En la sección 3.3.1 construiremos este diseño utilizando dichas matrices.

Acabamos de ver los parámetros que podría tener un diseño si v toma los valores extremos de la desigualdad pero, ¿qué ocurre si ambos extremos coinciden?, es decir, ¿qué diseño se forma si el límite inferior y superior de la condición (2.8) son el mismo?

Si $n = 2$, se cumple que $4n - 1 = 7 = n^2 + n + 1$ y, de este modo $v = 7$, obteniendo así un $2 - (7, 3, 1)$ diseño. En particular, este diseño se corresponde con el *Plano de Fano* y geométricamente, es el plano proyectivo finito con el menor número posible de puntos y rectas. Sin entrar en detalle sobre la construcción proyectiva de este diseño, veremos el conjunto de elementos y bloques que lo forman. Está constituido sobre el espacio vectorial $\mathbb{Z}_2^3$ y los siete puntos, excluyendo el $(0, 0, 0)$, se representan de la siguiente manera:

$$(0,0,1) \quad (0,1,0) \quad (1,0,0) \quad (0,1,1) \quad (1,0,1) \quad (1,1,0) \quad (1,1,1)$$

Si observamos la figura 2.1, es fácil comprobar que cada recta del plano tiene tres puntos, que por cada punto del plano pasan tres rectas y que por cada par de puntos pasa una única recta. Si identificamos los puntos como elementos y las rectas como bloques obtenemos el diseño formado por el conjunto de

elementos $X = \{1, 2, 3, 4, 5, 6, 7\}$ y el conjunto de bloques $B = \{\{1, 2, 5\}, \{1, 3, 6\}, \{1, 4, 7\}, \{2, 3, 7\}, \{3, 4, 5\}, \{5, 6, 7\}, \{2, 4, 6\}\}$.

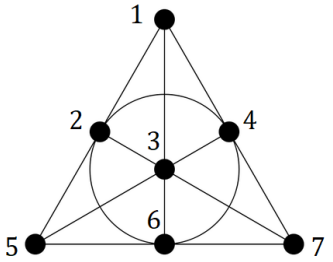

Figura 2.1: Plano de Fano

Además, este diseño es también un sistema triple de Steiner.

El siguiente teorema nos proporciona dos condiciones necesarias pero no suficientes para la existencia de diseños simétricos.

Teorema 2.32 ***(Teorema de Bruck-Ryser-Chowla)*** *Si existe un diseño simétrico con parámetros* $2 - (v, k, \lambda)$*, entonces:*

1. *Si* v *es par, el orden del diseño,* $k - \lambda$*, es un cuadrado.*
2. *Si* v *es impar, entonces existen tres números enteros* x, y, z *no nulos tal que* $x^2 = (k - \lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda z^2$.

Demostración: Sea $2 - (v, k, \lambda)$ un diseño simétrico. Distingamos dos casos:
1. Supongamos que v es par. Por ser un diseño simétrico, su matriz de incidencia A es cuadrada, es decir, se cumple que $|A| = |A^T|$, y de esta forma aplicando un resultado obtenido en la demostración del teorema 2.19 se obtiene que

$$|AA^T| = |A||A^T| = |A|^2 = rk(r - \lambda)^{v-1}.$$

De nuevo, por ser un diseño simétrico, se cumple que $r = k$, y así podemos reescribir la expresión anterior obteniendo que $|A|^2 = k^2(k - \lambda)^{v-1}$, esto es, $|A| = \pm k\sqrt{(k - \lambda)^{v-1}}$.
La matriz A es una matriz de números enteros, luego su determinante es un número entero. Como k y λ también son números enteros, $\sqrt{(k - \lambda)^{v-1}}$ ha de ser un número entero y por tanto, $(k - \lambda)^{v-1}$ es un cuadrado. Podemos concluir entonces que si v un número par, $(k - \lambda)$ es un cuadrado.

2. Supongamos ahora que v es impar. En virtud del Teorema de Lagrange [16] se tiene que

$$k - \lambda = a^2 + b^2 + c^2 + d^2,$$

con a, b, c y d enteros no negativos. Consideremos la matriz

$$B = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

y el producto

$$BB^T = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \begin{pmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{pmatrix}$$

que cumple que $BB^T = (a^2+b^2+c^2+d^2)I = (k-\lambda)I$. Por tanto, se tiene que $|BB^T| = (k-\lambda)^4$ y por ser B una matriz cuadrada, $|B|^2 = (k-\lambda)^4$, esto es, $|B| = (k-\lambda)^2$. Como esta expresión es distinta de cero la matriz B es no singular.
Sea $W = (w_1, w_2, w_3, w_4)$ cualquier vector columna de longitud 4 y sea $U = BW$. De esta forma, $U^TU = (BW)^T(BW) = W^TB^TBW$, es decir:

$$\begin{aligned} u_1^2 + u_2^2 + u_3^2 + u_4^2 &= (a^2+b^2+c^2+d^2)(w_1^2 + w_2^2 + w_3^2 + w_4^2) \\ &= (k-\lambda)(w_1^2 + w_2^2 + w_3^2 + w_4^2). \end{aligned} \tag{2.9}$$

Tomemos la matriz A de incidencia del diseño simétrico. A partir de esta vamos a definir las funciones $A_1, A_2, ..., A_v$ que dependerán del vector fila $X = (x_1, x_2, ..., x_v)$:

$$\begin{pmatrix} x_1, & x_2, & \cdots, & x_v \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1v} \\ a_{21} & a_{22} & \cdots & a_{2v} \\ \vdots & \vdots & & \vdots \\ a_{v1} & a_{v2} & \cdots & a_{vv} \end{pmatrix} = \begin{pmatrix} A_1, & A_2, & \cdots, & A_v \end{pmatrix}$$

esto es, cada $A_j = x_1a_{1j} + x_2a_{2j} + ... + x_va_{vj}$ es una aplicación lineal homogénea de $\mathbb{R}^v \longrightarrow \mathbb{R}$:

$$A_j = A_j(X) = \sum_{i=1}^{v} x_i a_{ij}. \tag{2.10}$$

De esta forma obtenemos que $XAA^TX^T = \sum_{j=1}^{v} A_j^2$.
Por otro lado, aplicando el teorema 2.18 a nuestro diseño simétrico, sabemos que $AA^T = (r-\lambda)I + \lambda J_{v\times v} = (k-\lambda)I + \lambda J_{v\times v}$, donde $J_{v\times v}$ es una matriz con todos los elementos iguales a uno. Multiplicando por X^T a la derecha y por X a la izquierda de esta ecuación obtenemos:

$$XAA^TX^T = (k-\lambda)XX^T + \lambda XJX^T.$$

Igualando ambas expresiones del producto XAA^TX^T, llegamos a la siguiente:

$$\sum_{j=1}^{v} A_j^2 = (k-\lambda)XX^T + \lambda XJX^T = (k-\lambda)\sum_{j=1}^{v} x_j^2 + \lambda(\sum_{j=1}^{v} x_j)^2. \tag{2.11}$$

Supongamos que $v \equiv 1 \pmod 4$. Definamos el conjunto de variables $y_1, y_2, ..., y_v$ tal que:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = B \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \begin{pmatrix} y_5 \\ y_6 \\ y_7 \\ y_8 \end{pmatrix} = B \begin{pmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}, ..., \begin{pmatrix} y_{v-4} \\ y_{v-3} \\ y_{v-2} \\ y_{v-1} \end{pmatrix} = B \begin{pmatrix} x_{v-4} \\ x_{v-3} \\ x_{v-2} \\ x_{v-1} \end{pmatrix}, y_v = x_v. \tag{2.12}$$

De la expresión (2.9), si $U = Y$ y $W = X$, obtenemos que $\sum_{j=1}^{v-1} y_j^2 = (k-\lambda)\sum_{j=1}^{v-1} x_j^2$ y de este modo la ecuación (2.11) se puede escribir como:

$$\sum_{j=1}^{v} A_j^2 = \sum_{j=1}^{v-1} y_j^2 + (k-\lambda)y_v^2 + \lambda(\sum_{j=1}^{v} x_j)^2. \tag{2.13}$$

Si nos fijamos en la expresión (2.12), las variables $y_1, y_2, ..., y_v$ han sido definidas en función de las variables $x_1, x_2, ..., x_v$. Pero por ser B una matriz no singular, posee matriz inversa y, de este modo, podemos escribir las variables $x_1, x_2, ..., x_v$ en función de las variables $y_1, y_2, ..., y_v$:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = B^{-1} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}, \begin{pmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} = B^{-1} \begin{pmatrix} y_5 \\ y_6 \\ y_7 \\ y_8 \end{pmatrix}, ..., \begin{pmatrix} x_{v-4} \\ x_{v-3} \\ x_{v-2} \\ x_{v-1} \end{pmatrix} = B^{-1} \begin{pmatrix} y_{v-4} \\ y_{v-3} \\ y_{v-2} \\ y_{v-1} \end{pmatrix}, x_v = y_v. \tag{2.14}$$

Como cada elemento x_i es una función lineal racional de y_i, de la expresión (2.10) es fácil ver que el elemento A_1 también es una función lineal racional de y_i:

$$A_1 = \sum_{i=1}^{v} e_i y_i, \tag{2.15}$$

donde cada elemento e_i es un número racional.
Además, de la expresión (2.14) se deduce que mediante la elección adecuada de las variables x_i, podemos obtener los valores que queramos de las variables y_j. Tomemos, por ejemplo, el valor

$$y_1 = \begin{cases} (-1-e_1)^{-1} \sum_{i=2}^{v} e_i y_i & \text{si } e_1 = 1 \\ \\ (1-e_1)^{-1} \sum_{i=2}^{v} e_i y_i & \text{en caso contrario} \end{cases} \tag{2.16}$$

De esta forma, una vez fijados los valores $x_2, x_3, ..., x_v$, el valor de y_1 queda unívocamente determinado por un único valor de x_1. Con ello, de las expresiones (2.15) y (2.16) obtenemos:

$$\begin{aligned} A_1^2 &= (e_1y_1 + e_2y_2 + ... + e_vy_v)^2 = (e_1\frac{1}{(1-e_1)}(e_2y_2 + e_3y_3 + ... + e_vy_v) + e_2y_2 + ... + e_vy_v)^2 = ... \\ ... &= (\frac{1}{(1-e_1)}(e_2y_2 + e_3y_3 + ... + e_vy_v))^2 = y_1^2, \end{aligned} \tag{2.17}$$

y así la ecuación (2.13) se puede simplificar obteniendo:

$$\sum_{j=2}^{v} A_j^2 = \sum_{j=2}^{v-1} y_j^2 + (k-\lambda)y_v^2 + \lambda(\sum_{j=1}^{v} x_j)^2. \tag{2.18}$$

Ahora, sabemos que cada función A_j para todo $1 \leq j \leq v$ y $\sum_{j=1}^{v} x_j$ son funciones lineales que dependen de las variables $x_1, x_2, ..., x_v$, y que estas a su vez, dependen de las variables $y_1, y_2, ..., y_v$. Además, la

variable y_1 es una función lineal homogénea que depende de las variables $y_2, y_3..., y_v$. Por lo tanto, cada función A_j y $\sum_{j=1}^{v} x_j$ se pueden considerar como funciones lineales homogéneas que dependen de las variables $y_2, y_3..., y_v$.

Siguiendo el procedimiento anterior para las funciones $A_2, A_3, ..., A_{v-1}$ y las variables $y_2, y_3, ..., y_{v-1}$ obtenemos que la ecuación (2.18) queda de la forma:

$$A_v^2 = (k-\lambda)y_v^2 + \lambda(\sum_{j=1}^{v} x_j)^2. \tag{2.19}$$

Así, para cualesquiera números racionales $\frac{p}{q}$ y $\frac{r}{s}$ podemos escribir $A_v = \frac{p}{q}y_v$ y $\sum_{j=1}^{v} x_j = \frac{r}{s}y_v$.

Si damos a y_v un valor, por ejemplo $y_v = qs$, y sustituimos en la ecuación (2.19) obtenemos:

$$(\frac{p}{q}qs)^2 = (k-\lambda)(qs)^2 + \lambda(\frac{r}{s}qs)^2,$$

esto es,

$$(ps)^2 = (k-\lambda)(qs)^2 + \lambda(rq)^2.$$

Por tanto, hemos conseguido números enteros $x = ps$, $y = qs$ y $z = rq$ tales que

$$x^2 = (k-\lambda)y^2 + \lambda z^2,$$

es decir,

$$x^2 = (k-\lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda z^2, \tag{2.20}$$

ya que $v \equiv 1 \pmod 4$ y con ello $(-1)^{\frac{v-1}{2}} = 1$.

Supongamos ahora que $v \equiv 3 \pmod 4$. Entonces, introducimos al conjunto de variables del caso anterior una nueva; x_{v+1} y de esta forma:

$$\begin{pmatrix} y_{v-2} \\ y_{v-1} \\ y_v \\ y_{v+1} \end{pmatrix} = B \begin{pmatrix} x_{v-2} \\ x_{v-1} \\ x_v \\ x_{v+1} \end{pmatrix}$$

Ahora, añadiendo el valor $(k-\lambda)x_{v+1}^2$ a ambos lados de la ecuación (2.13) y teniendo en cuenta que $(k-\lambda)\sum_{j=1}^{v+1} x_j^2 = \sum_{j=1}^{v+1} y_j^2$, se cumple:

$$\sum_{j=1}^{v} A_j^2 + (k-\lambda)x_{v+1}^2 = \sum_{j=1}^{v} y_j^2 + y_{v+1}^2 + \lambda(\sum_{j=1}^{v} x_j)^2. \tag{2.21}$$

Como la función A_1 depende de las variables $y_2, y_3, ..., y_v$, la función A_2 depende de las variables $y_3, y_4, ..., y_v$, y así sucesivamente hasta la función A_v que depende de la variable y_{v+1}, podemos simplificar la ecuación anterior obteniendo:

$$y_{v+1}^2 = (k-\lambda)x_{v+1}^2 - \lambda(\sum_{j=1}^{v} x_j)^2. \tag{2.22}$$

Por lo tanto, para cualesquiera números racionales $\frac{p}{q}$ y $\frac{r}{s}$ podemos escribir $x_{v+1} = \frac{p}{q}y_{v+1}$ y $\sum_{j=1}^{v} x_j = \frac{r}{s}y_{v+1}$. Si tomamos $y_{v+1} = qs$, sustituyendo en la ecuación (2.22) obtenemos:

$$(qs)^2 = (k-\lambda)(\frac{p}{q}qs)^2 - \lambda(\frac{r}{s}qs)^2,$$

esto es,

$$(qs)^2 = (k-\lambda)(ps)^2 - \lambda(rq)^2.$$

En consecuencia, hemos conseguido números enteros $x = qs$, $y = ps$ y $z = rq$ tales que

$$x^2 = (k-\lambda)y^2 - \lambda z^2,$$

es decir,

$$x^2 = (k-\lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda z^2, \tag{2.23}$$

ya que $v \equiv 3 \pmod 4$ y con ello $(-1)^{\frac{v-1}{2}} = -1$. □

Como vamos a ver en los siguientes ejemplos, este teorema permite descartar algunos parámetros como posibles $2-$diseños simétricos.

Ejemplo 16 *Aplicación del Teorema de Bruck-Ryser-Chowla:*

I) *Supongamos que existe un* $2-(22,7,2)$ *diseño. Se puede observar que se cumple que* $2(22-1) = 7(7-1)$*, es decir, si el diseño existe, es un diseño simétrico.*
Pero v *es par y* $k-\lambda = 5$ *no es un cuadrado. Luego por el Teorema de Bruck-Ryser-Chowla, no existe un diseño simétrico con parámetros* $2-(22,7,2)$*.*

II) *Supongamos ahora que existe un* $2-(141,21,3)$ *diseño. De nuevo, se cumple que* $3(141-1) = 21(21-1)$*, luego si el diseño existe, es un diseño simétrico.*
Por el Teorema de Bruck-Ryser-Chowla, como v *es impar, si existe un diseño con esos parámetros entonces existen enteros* x, y, z *distintos de cero tal que:*

$$x^2 = 18y^2 + 3z^2.$$

Supongamos, sin pérdida de generalidad, que x, y, z *no tienen ningún factor en común. Claramente,* 3 *debe de dividir a* x^2*, luego* 3 *divide a* x*, es decir,* $x = 3a$*. De este modo*

$$9a^2 = 18y^2 + 3z^2.$$

Así, z *ha de ser divisible también por* 3*, es decir, si* $z = 3b$ *se obtiene que*

$$9a^2 = 18y^2 + 27b^2$$

y por lo tanto,

$$a^2 = 2y^2 + 3b^2.$$

Si reducimos dicha ecuación módulo 3 *obtenemos que* $a^2 \equiv 2y^2 \pmod 3$*. Ahora, si* y *no es divisible por* 3*, entonces* $a^2 = 2y^2 \equiv 2 \pmod 3$*. Y no existe entero tal que su cuadrado sea* 2*.*
De esta forma, 3 *divide al elemento* y *y los enteros* x, y, z *tienen un factor en común. Que es absurdo. En consecuencia, no existe un diseño simétrico con parámetros* $2-(141,21,3)$*.*

2.3.2. Diseños resolubles

Uno de los problemas más famosos en la teoría de los diseños combinatorios y, en particular, uno de los primeros ejemplos de diseños resolubles, fue el problema de las quince colegialas de Kirkman. En 1850, Thomas P.Kirkman [17] propuso el siguiente problema como la consulta número VI en el Diario de la dama y el caballero . El problema decía así:

"Quince señoritas de una escuela caminan de tres en tres durante siete días seguidos. Es necesario organizarlas diariamente para que no haya dos de ellas que caminen juntas más de una vez en la misma semana."

Desde sus inicios, el problema despertó un gran interés entre los matemáticos. La primera solución fue publicada por Cayley [6] y años después Kirkman [18] dió su solución como un caso especial de los resultados contenidos en su primer artículo. De hecho, se sabe que existen siete soluciones no isomorfas de este problema (se pueden ver en la referencia [8]).

De manera equivalente, el problema consiste en organizar a las quince colegialas, cada uno de los siete días de la semana, en cinco filas por grupos de tres de forma que, al final de dichos días, cada pareja de señoritas hayan salido exactamente una vez juntas en algún grupo.

Con lo visto hasta ahora, si denotamos a las niñas como elementos y a las filas como bloques, debemos tomar 35 bloques de tamaño tres de un conjunto de quince elementos. Cada elemento se repetirá en siete bloques y cada par de elementos aparecerá en un bloque, es decir, buscamos solución de un $2-(15,3,1)$ diseño. Además, los 35 bloques deberán poder distribuirse en siete clases (días de la semana) de forma que cada día haya cinco bloques a los que pertenezcan todos los elementos una única vez. Una posible solución a este problema es la siguiente:

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
$\{1,2,3\}$	$\{1,4,7\}$	$\{1,5,15\}$	$\{1,9,13\}$	$\{1,6,10\}$	$\{1,8,11\}$	$\{1,12,14\}$
$\{4,5,6\}$	$\{2,5,8\}$	$\{2,9,10\}$	$\{2,4,12\}$	$\{2,11,15\}$	$\{2,7,14\}$	$\{2,6,13\}$
$\{7,8,9\}$	$\{3,10,13\}$	$\{3,4,14\}$	$\{3,5,11\}$	$\{3,7,12\}$	$\{3,6,9\}$	$\{3,8,15\}$
$\{10,11,12\}$	$\{6,11,14\}$	$\{6,8,12\}$	$\{6,7,15\}$	$\{4,8,13\}$	$\{4,10,15\}$	$\{4,9,11\}$
$\{13,14,15\}$	$\{9,12,15\}$	$\{7,11,13\}$	$\{8,10,14\}$	$\{5,9,14\}$	$\{5,12,13\}$	$\{5,7,10\}$

Acabamos de ver uno de los ejemplos más conocidos sobre diseños resolubles, pero se pueden plantear muchos más problemas que surgen en la vida cotidiana o en el diseño experimental que necesitan una solución.

Definición 2.33 *Un $2-$diseño (X,B) se puede resolver si sus bloques se pueden dividir en r subconjuntos R_1,...,R_r, llamados clases paralelas, donde cada subconjunto R_i contiene bloques disjuntos dos a dos y cuya unión es igual a todo el conjunto X.*

Ejemplo 17 *Sea el diseño de parámetros $2-(9,3,1)$ formado por el siguiente conjunto de bloques:*

$$\begin{array}{cccc} \{1,2,3\} & \{1,4,7\} & \{1,6,9\} & \{1,5,8\} \\ \{4,5,6\} & \{2,5,9\} & \{2,4,8\} & \{2,6,7\} \\ \underbrace{\{7,8,9\}}_{R_1} & \underbrace{\{3,6,8\}}_{R_2} & \underbrace{\{3,5,7\}}_{R_3} & \underbrace{\{3,4,9\}}_{R_4} \end{array}$$

Rápidamente se observa la división mostrada en cuatro clases paralelas R_i para $i=1,2,3,4$. Por lo tanto, el diseño de parámetros $2-(9,3,1)$ es resoluble. En concreto, este diseño es una posible solución al primer problema planteado en la introducción. Basta identificar los elementos como los nueve niños y las clases paralelas como los cuatro días en los que organizamos las actividades.

La siguiente desigualdad muestra una condición necesaria para la existencia de diseños resolubles.

Teorema 2.34 ***(Desigualdad de Bose, 1942)*** *[4] En todo $2-(v,k,\lambda)$ diseño resoluble con b bloques, se cumple que $b \geq v + r - 1$.*

Demostración: Sea un $2-(v,k,\lambda)$ diseño resoluble. Por ser un diseño resoluble, sus bloques se pueden dividir en r clases paralelas $R_i = \{B_{i_1}, ..., B_{i_n}\}$ con $i = 0, ..., r-1$, tal que cada una de ellas contiene exactamente a n bloques disjuntos entre sí y a todos los elementos del conjunto. De esta forma, $v = nk$ y $b = nr$.

Sea B_{0_1} uno de los bloques del diseño. Definimos l_{ij} como el número de elementos que tiene dicho bloque en común con el resto de bloques del diseño, es decir, $l_{ij} = |B_{0_1} \cap B_{i_j}|$ para $i = 1, 2, ..., r-1$ y $j = 1, 2, ..., n$, y por tanto el número de elementos l_{ij} es precisamente $n(r-1)$. Definamos ahora m como la media de los valores l_{ij}:

$$m = \frac{1}{n(r-1)} \sum_{i,j} l_{ij}. \tag{2.24}$$

Sabemos que cada uno de los k elementos que pertenecen al bloque B_{0_1} está en r bloques del diseño, por lo tanto cada uno de ellos estará en $(r-1)$ de los bloques restantes B_{i_j}. De este modo, $\sum_{i,j} l_{ij} = k(r-1)$.

Ahora, sustituyendo esta expresión en la ecuación (2.24) y teniendo en cuenta que $v = nk$, obtenemos

$$m = \frac{k}{n} = \frac{k^2}{v}. \tag{2.25}$$

Consideremos ahora la varianza σ^2 de cada elemento l_{ij}, esto es:

$$\sigma^2 = \frac{1}{n(r-1)} \sum_{i,j} (l_{ij} - m)^2 = \left(\frac{1}{n(r-1)} \sum_{i,j} l_{ij}^2 \right) - m^2. \tag{2.26}$$

Basta ver entonces cuál es el valor de $\sum_{i,j} l_{ij}^2$. Veamos que se cumple la siguiente ecuación:

$$\sum_{i,j} \frac{l_{ij}(l_{ij}-1)}{2} = (\lambda - 1)\frac{k(k-1)}{2}. \tag{2.27}$$

Para ello, vamos a calcular el numéro de bloques del diseño a los que pertenece cada pareja de elementos de B_{0_1}.

Por un lado, el bloque B_{0_1} tiene k elementos, luego hay $\binom{k}{2}$ opciones de escoger una pareja de elementos. Como dicha pareja ya pertenece al bloque B_{0_1}, estará en $(\lambda - 1)$ de los bloques restantes. Esto es, cada pareja de elementos pertenece a $(\lambda - 1)\frac{k(k-1)}{2}$ bloques del diseño.

Por otro lado, hay $\frac{l_{ij}(l_{ij}-1)}{2}$ formas de elegir dos elementos que estén a la vez en el bloque B_{0_1} y en el bloque B_{ij} para un i, j en particular. De esta forma, hay en total $\sum \frac{l_{ij}(l_{ij}-1)}{2}$ bloques que contienen a ese par de elementos.
Con esto, hemos probado que se cumple la expresión de la ecuación (2.27). De ella, teniendo en cuenta que $\lambda(v-1) = r(k-1)$ por ser un $2-$diseño, el valor de la suma de los l_{ij} calculado anteriormente y que $v = nk$, resulta la siguiente:

$$\sum_{i,j} l_{ij}^2 = \frac{k[(nk-1)(r-k) + r(k-1)^2]}{nk-1}. \tag{2.28}$$

Por lo tanto, si sustituimos las ecuaciones (2.24) y (2.28) en la ecuación (2.26), donde $b = nk$, se obtiene que:

$$\sigma^2 = \frac{k(v-k)(b-v-r+1)}{n^2(r-1)(v-1)}. \tag{2.29}$$

Teniendo en cuenta que la varianza de una variable es siempre mayor o igual que cero y que tanto las variables como los valores $(v-k)$, $(r-1)$ y $(v-1)$ son positivos, $(b-v-r+1)$ ha de ser mayor o igual que cero, es decir, $b \geq v+r-1$. □

Esta desigualdad nos proporciona una condición necesaria, pero no suficiente, que cumple todo $2-$diseño resoluble. En particular, es fácil observar que la expresión $b \geq v+r-1$ es equivalente a que se cumpla la desigualdad $r \geq k+\lambda$. En efecto, teniendo en cuenta que el número de bloques de un diseño es $b = \frac{vr}{k}$ y que en todo $2-$diseño $r = \lambda\frac{v-1}{k-1}$, se tiene que:

$$b \geq v+r-1 \Longleftrightarrow \tfrac{vr}{k} \geq v+r-1 \Longleftrightarrow \tfrac{v(r-k)}{k} \geq r-1 \Longleftrightarrow$$

$$\Longleftrightarrow v \geq \tfrac{k(r-1)}{r-k} \Longleftrightarrow \tfrac{r(k-1)+\lambda}{\lambda} \geq \tfrac{k(r-1)}{r-k} \Longleftrightarrow$$

$$\Longleftrightarrow r(k-1)(r-k)+\lambda(r-k) \geq \lambda k(r-1) \Longleftrightarrow$$

$$\Longleftrightarrow r(k-1)(r-k) \geq \lambda r(k-1) \Longleftrightarrow r-k \geq \lambda.$$

No obstante, esta condición no es suficiente, como se muestra a continuación con un pequeño ejemplo.

Ejemplo 18 *El diseño con parámetros* $2-(6,3,2)$ *y formado por el siguiente conjunto de bloques:*

$$\begin{array}{lllll} \{1,2,3\}, & \{1,3,5\}, & \{1,5,6\}, & \{2,4,5\}, & \{3,4,5\}, \\ \{1,2,4\}, & \{1,4,6\}, & \{2,3,6\}, & \{2,5,6\}, & \{3,4,6\}, \end{array}$$

cumple la condición $b \geq v+r-1$ *pero no es posible dividir los bloques del diseño en clases paralelas de forma que cada clase contenga bloques disjuntos dos a dos y cuya unión sea igual al conjunto total. Por lo tanto, no es un diseño resoluble.*

En la introducción se mencionó que los diseños, en algunos casos, tienen como aplicación resolver problemas que involucran el diseño de competiciones. Por ejemplo, si queremos organizar un torneo de tenis con $2n$ participantes de forma que cada uno juegue exactamente una vez contra todos los demás jugadores. Además, se pretende realizar la competición durante $2n-1$ días, de manera que en cada uno de ellos todos los participantes jueguen un partido con sus respectivos contrincantes. Para resolver este problema, debemos construir un $2-(2n,2,1)$ diseño resoluble. En particular, existe el siguiente resultado:

Teorema 2.35 *Para todo entero positivo* n*, existe un* $2-(2n,2,1)$ *diseño resoluble.*

Demostración: Sea el conjunto de elementos $X = \{0,1,2,...,2n-1\}$ y el conjunto B de bloques formado por los pares $\{a,b\}$ con $a \neq b$ y $a,b \in X$. Queremos ver que ambos conjuntos forman un diseño resoluble de parámetros $2-(2n,2,1)$.

Está claro que es un $2-(2n,2,1)$ diseño, ya que $|X| = 2n$, que cada bloque está formado por dos elementos y lógicamente, que cada par de elementos pertenece a un único bloque, que es el formado por ambos. Veamos entonces que dicho diseño es resoluble, es decir, que el conjunto de bloques se puede dividir en clases paralelas.

Sabemos que hay $\binom{2n}{n}$ posibles parejas de elementos, esto es, que el diseño está formado por $n(2n-1)$ bloques. Sean $R_1, R_2, ..., R_r$ las clases paralelas en las que se dividen estos. Como en cada clase tienen que estar todos los elementos del conjunto X y cada bloque tiene dos elementos, resulta que

$$2n \cdot r = 2 \cdot n(2n-1)$$

y, por lo tanto, hay $2n-1$ clases paralelas con bloques disjuntos dos a dos.

De esta forma, definimos cada clase R_i formada por los bloques $\{0, i\}$ y $\{a, b\}$ con $a+b \equiv 2i \pmod{2n-1}$ (n bloques en total), y tal que cada bloque aparece exactamente a una clase.

Vamos a ver que en cada una hay n bloques y para ello, bastará con ver que aparecen todos los elementos de X una única vez. Claramente, el elemento 0 e i están. Ahora, para cada elemento $j \in X \setminus \{0, i\}$, sea el elemento k con $k \equiv 2i - j \pmod{2n-1}$. Entonces, el bloque $\{j, k\}$ está en dicha clase paralela y dicho elemento no pertenece a ningún otro bloque de la misma clase. De lo contrario, si el bloque $\{j', k\}$ perteneciera a la misma clase paralela, se tendría que

$$k = 2i - j = 2i - j',$$

es decir, $j = j'$. Que es absurdo.

Por último, falta ver que cada bloque aparece en alguna clase. Distingamos dos casos:

- Si $a = 0$ o $b = 0$. Supongamos, por ejemplo, que $a = 0$. Si $a = 0$, entonces por definición, el bloque $\{0, b\}$ pertenece a la clase D_b. Análogamente para el caso $b = 0$.
- Si $a, b \neq 0$. Como $(2, 2n-1) = 1$, el bloque $\{a, b\}$ pertenecerá a la clase D_i con $i = \frac{a+b}{2} \pmod{2n-1}$ unívocamente determinado.

□

Capítulo 3

Construcciones de diseños

Hasta ahora hemos visto que podemos clasificar distintos tipos de diseños en función de las propiedades que cumplan sus parámetros. Por ejemplo, si cada conjunto de t elementos pertenece exactamente a un bloque del diseño, obtenemos los denominados sistemas de Steiner. Pero si, por otro lado, queremos que cada par de elementos pertenezca al mismo número de bloques de forma que se satisfagan ciertas condiciones, obtenemos los diseños simétricos y diseños resolubles. Además, se han probado diversos resultados en los que se obtienen nuevos diseños a partir de uno dado, como por ejemplo, los diseños residuales, los diseños derivados o los diseños complementarios.

El objetivo de este capítulo es abordar diversos métodos utilizados en la construcción de los diseños mencionados anteriormente. Para ello, utilizaremos distintos métodos como pueden ser los métodos de Skolem, el método de diferencias, matrices de Hadamard y geometría afín. Se han seguido las referencias [1], [2] y [23].

Cabe destacar que aparte de estas herramientas, existen muchos más métodos para la construcción de diseños combinatorios.

3.1. Construcción de sistemas triples de Steiner

En la sección de sistemas de Steiner y, en concreto, en el teorema 2.12, probamos una condición necesaria para la existencia de estos sistemas. Ahora, vamos a ver que dicha condición es también suficiente, es decir, si dado un $2-(v,3,1)$ diseño se cumple que $v \equiv 1$ o $3 \pmod 6$, entonces es un sistema triple de Steiner. De hecho, presentamos el método de Skolem, que permite construir sistemas triples de Steiner para algunos parámetros en concreto.

3.1.1. Método de Skolem para v=6n+3

Comencemos viendo el método desarrollado por Skolem para construir sistemas triples de Steiner con $v \equiv 3 \pmod 6$.

Teorema 3.1 *Sea $X = \{0, 1, 2, ..., 6n+2\}$ un conjunto con $v = 6n+3$ elementos. Consideremos a estos elementos en tres filas de $2n+1$ elementos cada una ordenados como sigue:*

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & \cdots & 2n\text{-}1 & 2n \\ 2n{+}1 & 2n{+}2 & 2n{+}3 & 2n{+}4 & \cdots & 4n & 4n{+}1 \\ 4n{+}2 & 4n{+}2 & 4n{+}4 & 4n{+}5 & \cdots & 6n{+}1 & 6n{+}2 \end{array} \tag{3.1}$$

de tal forma que la segunda, la tercera y la primera fila sean la siguiente a la primera, la segunda y la tercera respectivamente. Sea B el conjunto formado por los siguientes tipos de bloques:

1. $\{i, 2n+1+i, 4n+2+i\}$ *para* $0 \leq i \leq 2n$ *(elementos de una misma columna de* (3.1)*).*

2. $\{x, y, z\}$ *con* x, y *elementos de la misma fila y* z *un elemento de la siguiente fila a ambos tal que* $2z \equiv x + y \pmod{2n+1}$.

Entonces, el diseño (X, B) *es un sistema triple de Steiner de parámetros* $2-(v, 3, 1)$.

Demostración: Sea B el conjunto de bloques definido anteriormente. Está claro que cada bloque está formado por tres elementos. Comencemos viendo que el número de bloques que contiene el diseño es $b = \frac{v(v-1)}{6}$.
Por definición, hay $2n+1$ bloques del *Tipo 1.* Ahora, para cada bloque $\{x, y, z\}$ del *Tipo 2* podemos observar que el elemento z queda unívocamente determinado por los elementos x e y y que, además, no puede pertenecer a la misma columna que el elemento x o el elemento y. Supongamos que lo está, es decir, que $z \equiv x \pmod{2n+1}$. Entonces $2x \equiv x + y \pmod{2n+1}$, esto es, $x \equiv y \pmod{2n+1}$. Esto implica que x e y pertenecen a la misma columna y, por tanto, $x = y$ (ya que suponíamos que x e y estaban en la misma fila) que es absurdo.
De esta forma, hay $\binom{2n+1}{2} = n(2n+1)$ formas de escoger al par $\{x, y\}$ en cada fila y por tanto, $3 \cdot n(2n+1)$ bloques del *Tipo 2.*
Por lo tanto, el número total de bloques es

$$|B| = (2n+1) + 3n(2n+1) = \frac{v(v-1)}{6}$$

y así el conjunto B contiene el número de bloques que tiene todo sistema triple de Steiner. Ahora, falta ver que cada par de elementos distintos del conjunto X pertenece a un único bloque del conjunto B. Sean a y b dos elementos distintos de X. Consideremos tres casos:

- Si a y b están en la misma columna, está claro que solo pertenecen a un bloque del *Tipo 1.*
- Si a y b están en la misma fila, pertenecen por definición a un bloque del tipo *Tipo 2.* Este es único ya que de la ecuación $2c \equiv a+b \pmod{2n+1}$ el elemento c de dicho bloque, que pertenece a la siguiente fila de ambos, queda unívocamente determinado.
- Si a y b están en distinta fila y columna. En este caso podemos suponer que uno de ellos está en la siguiente fila del otro, por ejemplo, que b está en la siguiente fila a la que pertenece el elemento a, con $a \neq b \pmod{2n+1}$. Entonces a y b pertenecerán a un bloque del *Tipo 2* sí, y solo sí, existe un elemento d en la misma fila que a tal que $2b \equiv a + d \pmod{2n+1}$, esto es, tal que $d \equiv 2b - a \pmod{2n+1}$. Y está claro que este elemento es único y que además $d \neq a$. De lo contrario, si $a = d$, se tendría que $2a \equiv 2b \pmod{2n+1}$, es decir, que a y b estarían en la misma columna, que es absurdo.

De este modo, queda probado que el diseño (X, B) con $v = 6n+3$ así construido es un sistema triple de Steiner. □

Ejemplo 19 *Construcción de un sistema triple de Steiner con* $v = 21$.
Sabemos que $21 = 6 \cdot 3 + 3$*, luego* $n = 3$*. De esta forma, el conjunto* X *está formado por los siguientes elementos:*

0	*1*	*2*	*3*	*4*	*5*	*6*
7	*8*	*9*	*10*	*11*	*12*	*13*
14	*15*	*16*	*17*	*18*	*19*	*20*

Y el conjunto B estará formado por los siguientes bloques:

1. *De la forma $\{i, 2n+1+i, 4n+2+i\}$ para $0 \leq i \leq 2n$:*

$$\{0,7,14\},\quad \{1,8,15\},\quad \{2,9,16\},\quad \{3,10,17\},\quad \{4,11,18\},\quad \{5,12,19\},\quad \{6,13,20\}.$$

2. *De la forma $\{x, y, z\}$ con x, y elementos de la misma fila y z un elemento de la siguiente fila a ambos tal que $2z \equiv x + y \pmod{2n+1}$:*

$\{0,1,11\}$,	$\{1,2,12\}$,	$\{2,4,10\}$,	$\{3,14,20\}$,	$\{5,14,17\}$,	$\{7,11,16\}$,	$\{9,11,17\}$,
$\{0,2,8\}$,	$\{1,3,9\}$,	$\{2,5,7\}$,	$\{3,15,19\}$,	$\{5,15,16\}$,	$\{7,12,20\}$,	$\{9,12,14\}$,
$\{0,3,12\}$,	$\{1,4,13\}$,	$\{2,6,11\}$,	$\{3,16,18\}$,	$\{5,18,20\}$,	$\{7,13,17\}$,	$\{9,13,18\}$,
$\{0,4,9\}$,	$\{1,5,10\}$,	$\{2,14,18\}$,	$\{4,5,8\}$,	$\{6,14,19\}$,	$\{8,9,19\}$,	$\{10,11,14\}$,
$\{0,5,13\}$,	$\{1,6,7\}$,	$\{2,15,17\}$,	$\{4,6,12\}$,	$\{6,15,18\}$,	$\{8,10,16\}$,	$\{10,12,18\}$,
$\{0,6,10\}$,	$\{1,14,16\}$,	$\{2,19,20\}$,	$\{4,14,15\}$,	$\{6,16,17\}$,	$\{8,11,20\}$,	$\{10,13,15\}$,
$\{0,15,20\}$,	$\{1,17,20\}$,	$\{3,4,7\}$,	$\{4,16,20\}$,	$\{7,8,18\}$,	$\{8,12,17\}$,	$\{11,12,15\}$,
$\{0,16,19\}$,	$\{1,18,19\}$,	$\{3,5,11\}$,	$\{4,17,19\}$,	$\{7,9,15\}$,	$\{8,13,14\}$,	$\{11,13,19\}$,
$\{0,17,18\}$,	$\{2,3,13\}$,	$\{3,6,8\}$,	$\{5,6,9\}$,	$\{7,10,19\}$,	$\{9,10,20\}$,	$\{12,13,16\}$.

3.1.2. Método de Skolem para v=6n+1

De forma análoga al caso anterior, vamos a construir sistemas triples de Steiner con $v = 6n + 1$ utilizando el método desarrollado por Skolem.

Teorema 3.2 *Sea $X = \{0, 1, 2, ..., 6n\}$ un conjunto $v = 6n+1$ elementos el cual está formado por los elementos de las siguientes filas:*

$$\begin{array}{cccccc|cccc} 0 & 1 & 2 & \cdots & n\text{-}1 & & n & n{+}1 & \cdots & 2n\text{-}1 \\ 2n & 2n{+}1 & 2n{+}2 & \cdots & 3n\text{-}1 & & 3n & 3n{+}1 & \cdots & 4n\text{-}1 \\ 4n & 4n{+}1 & 4n{+}2 & \cdots & 5n\text{-}1 & & 5n & 5n{+}1 & \cdots & 6n\text{-}1 \end{array} \tag{3.2}$$

y el elemento $6n$. De igual forma, consideremos que la segunda, la tercera y la primera fila sean la siguiente a la primera, la segunda y la tercera respectivamente. Sea B el conjunto formado por los siguientes tipos de bloques:

1. *$\{i, 2n+i, 4n+i\}$ para $0 \leq i \leq n-1$ (en la misma columna de la parte izquierda de (3.2)).*

2. *$\{n+i, 2n+i, 6n\}$, $\{3n+i, 4n+i, 6n\}$, $\{5n+i, i, 6n\}$ para $0 \leq i \leq n-1$*
   (un elemento de la $i-$ésima columna de la parte izquierda de una fila, el elemento de la columna i de la parte derecha de la siguiente fila y el elemento $6n$).

3. *$\{x, y, z\}$ donde x, y son elementos de la misma fila y z es un elemento de la siguiente fila a ambos tal que:*

   3.1) Si $x + y$ es par, $2z \equiv x + y \pmod{2n}$ y z está en la mitad izquierda de la fila.

   3.2) Si $x + y$ es impar, $2z \equiv x + y - 1 \pmod{2n}$ y z está en la mitad derecha de la fila.

Entonces, el diseño (X, B) es un sistema triple de Steiner de parámetros $2-(v, 3, 1)$.

Demostración: Sea B el conjunto de bloques definidos anteriormente formado, cada uno, por tres elementos. De nuevo, comencemos viendo que el número de bloques que contiene el diseño es $b = \frac{v(v-1)}{6}$.

Por definición, hay n bloques del *Tipo 1* y $3n$ bloques del *Tipo 2*. Ahora, siguiendo el mismo razonamiento que para el caso $v = 6n + 3$, sabemos que hay $\binom{2n}{2}$ formas de escoger un par de elementos x, y en cada fila de forma que el elemento restante z del bloque quede unívocamente determinado. Luego hay $3 \cdot n(2n-1)$ bloques del *Tipo 3*. De esta forma, el número total de bloques es

$$|B| = n + 3n + 3n(2n-1) = n(6n+1) = \frac{v(v-1)}{6}.$$

Por tanto, el conjunto B contiene el número de bloques que tiene todo sistema triple de Steiner. Veamos ahora que cada par de elementos distintos del conjunto X están en un bloque de B. Sean a y b dos elementos distintos del conjunto $\{0, 1, 2, ..., 6n-1\}$. Consideremos los siguientes casos:

- Sea el par $\{a, 6n\}$. Por definición, el elemento $6n$ pertenece únicamente a los bloques del *Tipo 2* y aparece exactamente una vez con cada elemento restante del conjunto X. De este modo, el par $\{a, 6n\}$ aparece en un solo bloque del *Tipo 2*.

- Si a y b están en la misma columna, debemos distinguir dos casos:

  - Si están en la misma columna de la mitad izquierda, entonces por definición pertenecen a un bloque del *Tipo 1*. Veámos que solo pueden estar en un bloque de este tipo. Está claro que no pueden pertenecer a ningún bloque del *Tipo 2* ya que los elementos en estos bloques pertenecen a distintas columnas. Supongamos entonces que pertenecen a un bloque del *Tipo 3* con b situado en la siguiente fila a la del elemento a. Como b está en la mitad izquierda, el bloque ha de ser de la forma $\{a, d, b\}$ siendo d un elemento de la misma fila que a con $a \neq d$ y tal que $2b \equiv a + d \pmod{2n}$. Pero $a = b \pmod{2n}$ por estar en la misma columna, luego $a \equiv d \pmod{2n}$. Y esto absurdo porque estamos suponiendo que a y d están en la misma fila y son distintos, luego no pueden pertenecer a la misma columna.
    De esta forma queda probado que el par $\{a, b\}$ que satisface esas condiciones solo pertenece a un bloque del *Tipo 1*.
  - Si están en la misma columna de la mitad derecha. Supongamos que b está en la fila siguiente a la del elemento a. Es fácil ver que dicho par de elementos no pueden pertenecer a ningún bloque del *Tipo 1* ni del *Tipo 2*, luego han de pertenecer a algún bloque del *Tipo 3*. Como b está en la mitad derecha, el bloque tiene que ser de la forma $\{a, d, b\}$ siendo d un elemento de la misma fila que a con $a \neq d$ y tal que $2b \equiv a + d - 1 \pmod{2n}$. Como $a = b \pmod{2n}$ por estar en la misma columna, se tiene que $d \equiv a + 1 \pmod{2n}$, y por tanto el elemento d queda unívocamente determinado.

- Si a y b están en la misma fila, por definición han de pertenecer a algún bloque del *Tipo 3*. Y en este caso dicho bloque es único, ya que el elemento restante c del bloque queda únivocamente determinado.

- Si a y b están en distinta fila y columna. En este caso está claro que no pueden pertenecer a ningún bloque del *Tipo 1*. Supongamos de nuevo que b está en la fila siguiente a la del elemento a y distingamos los siguientes casos:

  - Si el elemento b está situado en la mitad izquierda y $b = a \pmod{n}$, entonces existe un único bloque del *Tipo 2* que contiene a este par de elementos. Además, no pertenecerán a ningún bloque del *Tipo 3* ya que entonces existiría un elemento d con $d \neq a$ tal que $2b \equiv a + d \pmod{2n}$. Y esto no es posible porque si $b = a \pmod{n}$, entonces $2b = 2a \pmod{2n}$ y así $a \equiv d \pmod{2n}$, que es absurdo.

- Si el elemento b está situado en la mitad izquierda y $b \neq a \pmod{n}$, entonces el par $\{a, b\}$ no puede estar contenido en ningún bloque del *Tipo 2*. Veamos que este par está contenido en un único bloque del *Tipo 3* de la forma $\{a, d, b\}$. Como el elemento b está situado en la parte izquierda de las filas, existirá un elemento d en la misma fila que a con $d \neq a$ tal que $2b \equiv a + d \pmod{2n}$, es decir, $d \equiv 2b - a \pmod{2n}$. De lo contrario, si $d = a$, se tendría que $2b \equiv 2a \pmod{2n}$, que es lo mismo que $b = a \pmod{n}$, llegando a un absurdo.
- Si el elemento b está situado en la mitad derecha, el par $\{a, b\}$ estará en un bloque del *Tipo 3*. Por estar en dicha parte, existirá un elemento d en la misma fila que a tal que $2b \equiv a + d - 1 \pmod{2n}$, esto es, $d \equiv 2b - a + 1 \pmod{2n}$. Además, d ha de ser distinto de a. De lo contrario $a + d$ sería par, que es absurdo ya que estamos suponiendo que b está en la mitad derecha de la fila.
  Por último, el par $\{a, b\}$ no estará en ningún bloque del *Tipo 2* por definición de estos. Si b perteneciera a alguno de estos bloques, el elemento a estaría en la siguiente fila a b, no en la anterior.

Por lo tanto, todo par de elementos del conjunto X pertenecen a un bloque del conjunto B. Podemos concluir entonces que el diseño (X, B) con $v = 6n + 1$ es un sistema triple de Steiner. □

Ejemplo 20 *Construcción de un sistema triple de Steiner con* $v = 19$.
Sabemos que $19 = 6 \cdot 3 + 1$, *luego* $n = 3$. *De esta forma, el conjunto* X *está formado por los siguientes elementos:*

0	*1*	*2*	*3*	*4*	*5*
6	*7*	*8*	*9*	*10*	*11*
12	*13*	*14*	*15*	*16*	*17*

y el elemento 18. Y el conjunto B *estará formado por los siguientes bloques:*

1. *De la forma* $\{i, 2n + i, 4n + i\}$ *para* $0 \leq i \leq n - 1$*:*

$$\{0, 6, 12\}, \quad \{1, 7, 13\}, \quad \{2, 8, 14\}.$$

2. *De la forma* $\{n + i, 2n + i, 6n\}$, $\{3n + i, 4n + i, 6n\}$, $\{5n + i, i, 6n\}$ *para* $0 \leq i \leq n - 1$*:*

$$\begin{array}{lll} \{0, 15, 18\}, & \{3, 6, 18\}, & \{9, 12, 18\}, \\ \{1, 16, 18\}, & \{4, 7, 18\}, & \{10, 13, 18\}, \\ \{2, 17, 18\}, & \{5, 8, 18\}, & \{11, 14, 18\}. \end{array}$$

3. *De la forma* $\{x, y, z\}$ *donde* x, y *son elementos de la misma fila y* z *es un elemento de la siguiente fila a ambos tal que:*

   3.1) Si $x + y$ *es par,* $2z \equiv x + y \pmod{2n}$ *y* z *está en la mitad izquierda de la fila.*

   3.2) Si $x + y$ *es impar,* $2z \equiv x + y - 1 \pmod{2n}$ *y* z *está en la mitad derecha de la fila.*

$$\begin{array}{lllllll} \{0, 1, 9\}, & \{1, 2, 10\}, & \{2, 4, 6\}, & \{3, 14, 17\}, & \{5, 13, 16\}, & \{7, 8, 16\}, & \{9, 10, 15\}, \\ \{0, 2, 7\}, & \{1, 3, 8\}, & \{2, 5, 9\}, & \{3, 15, 16\}, & \{5, 14, 15\}, & \{7, 9, 14\}, & \{9, 11, 13\}, \\ \{0, 3, 10\}, & \{1, 4, 11\}, & \{2, 12, 16\}, & \{4, 5, 10\}, & \{6, 7, 15\}, & \{7, 10, 17\}, & \{10, 11, 16\}. \\ \{0, 4, 8\}, & \{1, 5, 6\}, & \{2, 13, 15\}, & \{4, 12, 15\}, & \{6, 8, 13\}, & \{7, 11, 12\}, & \\ \{0, 5, 11\}, & \{1, 12, 14\}, & \{3, 4, 9\}, & \{4, 13, 14\}, & \{6, 9, 16\}, & \{8, 9, 17\}, & \\ \{0, 13, 17\}, & \{1, 15, 17\}, & \{3, 5, 7\}, & \{4, 16, 17\}, & \{6, 10, 14\}, & \{8, 10, 12\}, & \\ \{0, 14, 16\}, & \{2, 3, 11\}, & \{3, 12, 13\}, & \{5, 12, 17\}, & \{6, 11, 17\}, & \{8, 11, 15\}, & \end{array}$$

De este modo, por el teorema 2.12 y las dos construcciones anteriores, queda probado el siguiente teorema.

Teorema 3.3 *Un sistema triple de Steiner con parámetros* $2-(v,3,1)$ *existe sí, y solo sí,* $v \equiv 1$ *o* 3 (mód 6).

3.2. Construcción de diseños simétricos mediante métodos de diferencias

Para la construcción de diseños simétricos utilizaremos conjuntos de diferencias y en concreto, el conjunto de los residuos cuadráticos de un cuerpo finito, que no es más que un método de diferencias.

Definición 3.4 *Sea* $(G,+)$ *un grupo abeliano de orden* v*. Un* $(v,k,\lambda)-$*conjunto diferencia en* $(G,+)$ *es un* $k-$*subconjunto* $D \subseteq G$ *tal que el conjunto de todas las diferencias de los elementos de este conjunto expresan exactamente* λ *veces todo elemento de* G *no nulo. Es decir, todo elemento* $g \in G$ *distinto de cero puede expresarse exactamente* λ *veces como* $g = d_i - d_j$ *con* d_i *y dj elementos distintos de* D*.*

Además, si $D = \{d_1, d_2, ..., d_k\}$ es un conjunto diferencia, entonces el conjunto $D + g = \{d_1 + g, d_2 + g, ..., d_k + g\}$ también es un conjunto diferencia para todo elemento $g \in G$ distinto de cero. A estos conjuntos les llamaremos conjuntos trasladados de D.

En particular, como en el conjunto D hay $k(k-1)$ posibles diferencias y estas representan a cada uno de los $(v-1)$ elementos no nulos de G módulo v exactamente λ veces, si (v,k,λ) es un conjunto diferencia, entonces se cumple que $\lambda(v-1) = k(k-1)$.

Teorema 3.5 *Sea* $D = \{d_1, d_2, ..., d_k\}$ *un* (v,k,λ)*-conjunto diferencia sobre un grupo abeliano* $(G,+)$ *de orden* v*. Entonces, el conjunto* G *y el conjunto de bloques formado por todos los conjuntos trasladados de* D *forman un* $2-(v,k,\lambda)$ *diseño simétrico.*

Demostración: Sea $(G,+)$ un grupo abeliano de orden v y $D = \{d_1, d_2, ..., d_k\}$ un $(v,k,\lambda)-$conjunto diferencia sobre $(G,+)$. Si consideramos el conjunto G como el conjunto X de elementos del diseño y los conjuntos trasladados de D; D, $D+1$, ..., $D+(v-1)$ como los bloques del diseño, este estará formado por v elementos y cada bloque tendrá k de ellos. Por tanto, basta ver que todo par de elementos a, b de G pertenece al mismo número de bloques; λ.
Podemos expresar el elemento $a \in G$ como $a = d_i + (a - d_i)$ para todo $1 \leq i \leq k$, luego dicho elemento pertenecerá al bloque $D + (a - d_i)$. Análogamente, podemos expresar el elemento $b \in G$ como $b = d_j + (b - d_j)$ para todo $1 \leq j \leq k$ y de esta forma, pertenecerá al bloque $D + (b - d_j)$. Así, ambos elementos estarán en el mismo bloque $D + d$ si $d = a - d_i = b - d_j$ para algún $1 \leq i, j \leq k$.
Que se satisfaga la ecuación $a - d_i = b - d_j$ es equivalente a que se cumpla $a - b = d_i - d_j$ y, por definición de conjunto diferencia, sabemos que hay exactamente λ pares $\{i, j\}$ para los que se cumple que $d_i - d_j = a - b = d$. Por lo tanto, los elementos a y b aparecerán juntos en λ bloques del diseño, formando así un $2-(v,k,\lambda)$ diseño.
Además, por ser D un conjunto diferencia, este diseño es simétrico, ya que se cumple que $\lambda(v-1) = k(k-1)$. □

Ejemplo 21 *Sea el grupo aditivo* $(\mathbb{Z}/13\mathbb{Z}, +)$*. El conjunto* $D = \{1, 2, 4, 10\}$ *es un* $(13,4,1)$*-conjunto diferencia. Si calculamos todas las posibles diferencias del conjunto* D *obtenemos una vez todos los elementos del grupo* $\mathbb{Z}/13\mathbb{Z}$ *no nulos:*

$$\begin{array}{llll} 2-1=1 & 1-10=4 & 4-10=7 & 1-4=10 \\ 4-2=2 & 2-10=5 & 10-2=8 & 2-4=11 \\ 4-1=3 & 10-4=6 & 10-1=9 & 1-2=12 \end{array}$$

Además, si consideramos los conjuntos trasladados de $D=\{1,2,4,10\}$*:*

$$\begin{array}{lll} D+1=\{2,3,5,11\}, & D+5=\{2,6,7,9\}, & D+9=\{0,6,10,11\}, \\ D+2=\{3,4,6,12\}, & D+6=\{3,7,8,10\}, & D+10=\{1,7,11,12\}, \\ D+3=\{0,4,5,7\}, & D+7=\{4,8,9,11\}, & D+11=\{0,2,8,12\}, \\ D+4=\{1,5,6,8\}, & D+8=\{5,9,10,12\}, & D+12=\{0,1,3,9\}. \end{array}$$

obtenemos un $2-(13,4,1)$ *diseño simétrico formado por el conjunto* $X=\mathbb{Z}/13\mathbb{Z}$ *y por el conjunto de bloques los conjuntos trasladados de* D*.*

Una de las construcciones más importantes que utiliza conjuntos de diferencias es la construcción de Paley (1933). En ella se construyen conjuntos de diferencias a partir de los residuos cuadráticos de un cuerpo finito $\mathbb{F}_q$. Estos residuos cuadráticos serán precisamente todas las potencias pares de cualquier elemento primitivo de dicho cuerpo.

Teorema 3.6 *Sea* $\mathbb{F}_q$ *un cuerpo con* $q\equiv 3$ (mód 4) *potencia de un número primo y sea* Q *el conjunto de todos los cuadrados de* $\mathbb{F}_q$ *distintos de cero. Entonces, el diseño formado por todos los elementos de* $\mathbb{F}_q$ *y por el conjunto de bloques formado por todos los conjuntos trasladados de* Q *es un* $2-(q,\frac{q-1}{2},\frac{q-3}{4})$ *diseño simétrico.*

Demostración: Sea $\mathbb{F}_q$ un cuerpo finito con $q\equiv 3$ (mód 4) potencia de un número primo y sea θ un elemento primitivo de este cuerpo. De este modo, podemos escribir los cuadrados distintos de cero de $\mathbb{F}_q$ como las potencias pares del elemento θ.

Como $q=4t+3$, el elemento $-1\notin Q$. De lo contrario, si $-1\in Q$, $-1=w^2$ y así $1=w^4$. Pero los elementos distintos de cero de $\mathbb{F}_q$ forman un grupo respecto de la operación producto, luego el orden de w debe de dividir al orden del grupo, es decir, 4 debe dividir a $(q-1)$. Que contradice que $q\equiv 3$ (mód 4).

Además, para cualquier elemento x de $\mathbb{F}_q^*$, tendremos que $x\in Q$ sí, y solo sí, $-x\notin Q$. De esta forma, para cada elemento $x\in\mathbb{F}_q^*$, x o $-x$ será un cuadrado y por lo tanto, la mitad de elementos de $\mathbb{F}_q$ serán cuadrados y la otra mitad serán no cuadrados. Ahora, como los residuos cuadráticos se pueden expresar de la forma θ^{2a} para $a=1,2,...,2t+1$ obtenemos el conjunto $Q=\{\theta^2,\theta^4,...,\theta^{4t+2}=1\}$ y el conjunto $-Q=\{\theta,\theta^3,...,\theta^{4t+1}\}$.

Veamos entonces que el conjunto Q formado por los cuadrados de $\mathbb{F}_q^*$ es un conjunto diferencia. Supongamos que 1 puede ser escrito como diferencia de cuadrados de Q tal que

$$1=\theta^{2a_1}-\theta^{2b_1}=...=\theta^{2a_\lambda}-\theta^{2b_\lambda}.$$

Así cualquier cuadrado de Q; $\theta^{2s}\in Q$, puede ser expresado como

$$\theta^{2s}=\theta^{2(a_1+s)}-\theta^{2(b_1+s)}=...=\theta^{2(a_\lambda+s)}-\theta^{2(b_\lambda+s)}.$$

Análogamente, podemos observar que si cualquier cuadrado de Q puede ser expresado como diferencia de cuadrados de Q

$$\theta^{2r}=\theta^{2c_1}-\theta^{2d_1}=...=\theta^{2c_\lambda}-\theta^{2d_\lambda},$$

entonces el elemento 1 también puede ser expresado como tal del mismo número de formas

$$1 = \theta^{2(c_1-r)} - \theta^{2(d_1-r)} = ... = \theta^{2(c_\lambda-r)} - \theta^{2(d_\lambda-r)}.$$

De este modo, cada forma de expresar el número 1 proporciona una manera de representar cada cuadrado de $\mathbb{F}_q^*$ como diferencia de elementos de Q. Además, si $x \notin Q$, entonces $-x \in Q$ y toda representación de $-x = \theta^{2a} - \theta^{2b}$ como diferencia de cuadrados se corresponde con la diferencia $x = \theta^{2b} - \theta^{2a}$. Esto implica que todo elemento que no esté en Q, y que por tanto esté en $-Q$, tiene el mismo número de representaciones que un elemento que esté en el conjunto Q.

Por lo tanto, acabamos de ver que todo elemento de $\mathbb{F}_q^*$, sea cuadrado o no, se puede representar como diferencia de cuadrados, es decir, como diferencia de elementos de Q exactamente λ veces. Así, Q es un conjunto diferencia y aplicando el teorema 3.5 tenemos que el diseño formado por el conjunto de elementos de $\mathbb{F}_q$ y el conjunto de bloques formado por todos los conjuntos trasladados de Q forman un $2-(q,k,\lambda)$ diseño simétrico. Como $k = |Q| = \frac{q-1}{2}$ y se cumple que $\lambda(v-1) = k(k-1)$, obtenemos que $\lambda = \frac{q-3}{4}$. □

A partir del teorema anterior es fácil observar que el conjunto $-Q$ también es un conjunto diferencia y, por tanto, sus trasladados forman el conjunto de bloques de un diseño simétrico.

Corolario 3.7 *Sea $\mathbb{F}_q$ un cuerpo con $q \equiv 3$ (mód 4) potencia de un número primo y sea $-Q$ el conjunto formado por todos los residuos no cuadráticos de $\mathbb{F}_q$ y el elemento 0. Entonces, el diseño formado por todos los elementos de $\mathbb{F}_q$ y por el conjunto de bloques formado por todos los conjuntos trasladados de $-Q$ es un $2-(q, \frac{q+1}{2}, \frac{q+1}{4})$ diseño simétrico.*

Ejemplo 22 *Sea $\mathbb{F}_q$ un cuerpo con $q = 4 \cdot 4 + 3 = 19$ potencia de un número primo. Entonces, el conjunto de los residuos cuadráticos no nulos será el conjunto diferencia:*

$$\begin{array}{lllll} 1^2 = 1 & 3^2 = 9 & 5^2 = 6 & 7^2 = 11 & 9^2 = 5 \\ 2^2 = 4 & 4^2 = 16 & 6^2 = 17 & 8^2 = 7 & \end{array}$$

Así, el conjunto diferencia será $Q = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$.
Si consideramos los conjuntos trasladados de Q como bloques:

$$\begin{array}{ll} Q+1 = \{2,5,6,7,8,10,12,17,18\}, & Q+10 = \{0,2,7,8,11,14,15,16,17\}, \\ Q+2 = \{0,3,6,7,8,9,11,13,18\}, & Q+11 = \{1,3,8,9,12,15,16,17,18\}, \\ Q+3 = \{0,1,4,7,8,9,10,12,14\}, & Q+12 = \{0,2,4,9,10,13,16,17,18\}, \\ Q+4 = \{1,2,5,8,9,10,11,13,15\}, & Q+13 = \{0,1,3,5,10,11,14,17,18\}, \\ Q+5 = \{2,3,6,9,10,11,12,14,16\}, & Q+14 = \{0,1,2,4,6,11,12,15,18\}, \\ Q+6 = \{3,4,7,10,11,12,13,15,17\}, & Q+15 = \{0,1,2,3,5,7,12,13,16\}, \\ Q+7 = \{4,5,8,11,12,13,14,16,18\}, & Q+16 = \{1,2,3,4,6,8,13,14,17\}, \\ Q+8 = \{0,5,6,9,12,13,14,15,17\}, & Q+17 = \{2,3,4,5,7,9,14,15,18\}, \\ Q+9 = \{1,6,7,10,13,14,15,16,18\}, & Q+18 = \{0,3,4,5,6,8,10,15,16\}, \end{array}$$

obtenemos un $2-(19,9,4)$ diseño simétrico.
Además, si tomamos el conjunto de los residuos no cuadráticos de $\mathbb{F}_{19}$ y el elemento 0, es decir, el conjunto diferencia $-Q = \{0,2,3,8,10,12,13,14,15,18\}$, se obtiene un $2-(19,10,5)$ diseño simétrico:

$$-Q+1=\{0,1,3,4,9,11,13,14,15,16\},\quad -Q+10=\{1,3,4,5,6,9,10,12,13,18\},$$
$$-Q+2=\{1,2,4,5,10,12,14,15,16,17\},\quad -Q+11=\{0,2,4,5,6,7,10,11,13,14\},$$
$$-Q+3=\{2,3,5,6,11,13,15,16,17,18\},\quad -Q+12=\{1,3,5,6,7,8,11,12,14,15\},$$
$$-Q+4=\{0,3,4,6,7,12,14,16,17,18\},\quad -Q+13=\{2,4,6,7,8,9,12,13,15,16\},$$
$$-Q+5=\{0,1,4,5,7,8,13,15,17,18\},\quad -Q+14=\{3,5,7,8,9,10,13,14,16,17\},$$
$$-Q+6=\{0,1,2,5,6,8,9,14,16,18\},\quad -Q+15=\{4,6,8,9,10,11,14,15,17,18\},$$
$$-Q+7=\{0,1,2,3,6,7,9,10,15,17\},\quad -Q+16=\{0,5,7,9,10,11,12,15,16,18\},$$
$$-Q+8=\{1,2,3,4,7,8,10,11,16,18\},\quad -Q+17=\{0,1,6,8,10,11,12,13,16,17\},$$
$$-Q+9=\{0,2,3,4,5,8,9,11,12,17\},\quad -Q+18=\{1,2,7,9,11,12,13,14,17,18\},$$

formado por el mismo conjunto de elementos y el conjunto de bloques formado por los conjuntos trasladados de $-Q$.

Acabamos de probar la construcción de Paley utilizando que el conjunto de residuos cuadráticos de un cuerpo finito es un conjunto diferencia. Ahora, vamos a ver que es posible demostrar esta construcción sin utilizar este tipo de conjuntos. Para ello vamos a enunciar el siguiente lema, cuya demostración puede verse en [19].

Lema 3.8 *Sea q una potencia de un número primo, $b \in \mathbb{F}_q$, $a_1, a_2 \in \mathbb{F}_q^*$ y $\mathcal{X}$ la función característica siguiente (que es precisamente el símbolo de Legendre):*

$$\mathcal{X}(a) = \begin{cases} 1 & \text{si } a \text{ es un cuadrado} \\ 0 & \text{si } p \mid a \\ -1 & \text{si } a \text{ no es un cuadrado} \end{cases}$$

Entonces la ecuación $a_1x_1^2 + a_2x_2^2 = b$ tiene $q + V(b)\mathcal{X}(-a_1a_2)$ soluciones, donde $V(b) = -1$ si $b \in \mathbb{F}_q^*$ y $V(b) = q-1$ en caso contrario.

Teorema 3.9 *Sea $\mathbb{F}_q$ un cuerpo con $q \equiv 3$ (mód 4) potencia de un número primo y sea Q el conjunto de todos los cuadrados de $\mathbb{F}_q$ distintos de cero. Entonces, el diseño formado por todos los elementos de $\mathbb{F}_q$ y por el conjunto de bloques formado por todos los conjuntos de la forma $\{Q + a : a \in \mathbb{F}_q\}$ es un $2-(q, \frac{q-1}{2}, \frac{q-3}{4})$ diseño simétrico.*

Demostración: Sea $\mathbb{F}_q$ un cuerpo finito con $q \equiv 3$ (mód 4) potencia de un número primo. Como vimos anteriormente, para cada elemento $x \in \mathbb{F}_q^*$, x o $-x$ será un cuadrado. Por lo tanto, el conjunto Q tendrá $\frac{q-1}{2}$ elementos y en consecuencia, este será el número de elementos de todos los bloques del diseño. Para ver entonces que es un $2-$diseño, basta comprobar que todo par de elementos de $\mathbb{F}_q$ pertenece al mismo número de bloques. Sean x e y dos elementos distintos de $\mathbb{F}_q$, entonces:

$$|\{B_i \text{ bloque tal que } \{x,y\} \in B_i\}| = |\{a \in \mathbb{F}_q : \{x,y\} \in Q + a\}| =$$

$$= |\{a \in \mathbb{F}_q : x - a \in Q \text{ y } y - a \in Q\}| =$$

$$= |\{a \in \mathbb{F}_q : x - a = \alpha^2 \text{ y } y - a = \beta^2 \text{ con } \alpha, \beta \neq 0\}| =$$

$$= |\{(\alpha^2, \beta^2) \text{ tal que } \alpha^2 - \beta^2 = x - y \text{ con } \alpha, \beta \neq 0\}|.$$

Queremos ver cuántos pares hay de la forma (α^2, β^2) que satisfagan la ecuación $\alpha^2 - \beta^2 = x - y$ con $\alpha, \beta \neq 0$. Distingamos dos casos:

- Si $x - y \in Q$, es decir, si la diferencia $x - y$ es un cuadrado en $\mathbb{F}_q$, entonces $\mathcal{X}(x-y) = 1$. Además, $V(x-y) = -1$ y, aplicando el lema 3.8, obtenemos que la ecuación $\alpha^2 - \beta^2 = x - y$ tiene $q + (-1)\mathcal{X}(-1(-1)) = q + (-1)\mathcal{X}(1) = q - 1$ soluciones.
  Ahora, tenemos que ver qué ocurre en los casos en los que $\alpha = 0$ o $\beta = 0$. Si $\alpha = 0$, $-\beta^2 = x - y$ no tiene solución, ya que $-\beta^2$ no es un cuadrado por serlo β^2 y $(x-y)$ sí es un cuadrado. Por otro lado si $\beta = 0$, la ecuación $\alpha^2 = x - y$ tiene dos soluciones de la forma $(\pm\sqrt{x-y}, 0)$ que no debemos tener en cuenta, ya que estamos suponiendo $\beta \neq 0$. Además, las soluciones de la forma (α, β), $(-\alpha, \beta)$, $(\alpha, -\beta)$ y $(-\alpha, -\beta)$ nos darán el mismo par (α^2, β^2).
  Por lo tanto, habrá $\frac{q-3}{4}$ pares de la forma (α^2, β^2) que satisfagan la ecuación $\alpha^2 - \beta^2 = x - y$ con $\alpha, \beta \neq 0$.
- Si $x - y \notin Q$, es decir, si la diferencia $x - y$ no es un cuadrado en $\mathbb{F}_q$, entonces $\mathcal{X}(x-y) = -1$ y $V(x-y) = -1$. Siguiendo el mismo procedimiento que en el caso anterior, obtenemos que la ecuación $\alpha^2 - \beta^2 = x - y$ tiene $q - 1$ soluciones. En este caso, hemos de quitar las soluciones de la forma $(0, \pm\sqrt{x-y})$ y de nuevo, dividir entre cuatro el número de soluciones. De este modo, también habrá $\frac{q-3}{4}$ pares de la forma (α^2, β^2) que satisfagan la ecuación $\alpha^2 - \beta^2 = x - y$ con $\alpha, \beta \neq 0$.

Con esto, hemos probado que todo par de elementos distintos $x, y \in \mathbb{F}_q$ pertenece a $\frac{q-3}{4}$ bloques del diseño y podemos concluir, teniendo en cuenta que se cumple $\lambda(v-1) = k(k-1)$, que es un $2 - (q, \frac{q-1}{2}, \frac{q-3}{4})$ diseño simétrico. □

3.3. Construcción de otros t-diseños

En esta sección se mostrarán algunas construcciones de $t-$diseños utilizando distintas herramientas. En particular, utilizaremos matrices de Hadamard y geometría afín para construir 2 y 3−diseños.

3.3.1. Matrices de Hadamard

En la sección 2.3 introdujimos el concepto de diseño de Hadamard. Este no era más que un 2−diseño que contaba con el mismo número de elementos que el valor inferior de la desigualdad de la ecuación (2.8) que cumple todo diseño simétrico. Para probar estas construcciones necesitamos conocer antes algunas nociones básicas sobre las matrices de Hadamard.

Definición 3.10 *Una matriz H de tamaño $n \times n$ se denomina de Hadamard si está formada por elementos del conjunto $\{1, -1\}$ y cumple que $HH^T = nI_d$.*

Si se satisface la condición $HH^T = nI_d$, entonces también se cumple que $H^TH = nI_d$, es decir, si H es una matriz de Hadamard, su traspuesta H^T también es una matriz de Hadamard. Además, es fácil observar que la primera ecuación es equivalente a decir que todas las columnas de H han de ser ortogonales y, de la misma forma, la segunda ecuación es equivalente a decir que todas las filas de H han de ser ortogonales. Así, podemos afirmar que una matriz de tamaño $n \times n$ cuyas entradas son 1 o -1 es de Hadamard sí, y solo sí, sus filas y columnas son ortogonales dos a dos.

Entonces, cabe destacar que podemos multiplicar cualquier fila y cualquier columna de una matriz por -1 para obtener una matriz de Hadamard. En particular, diremos que una matriz de Hadamard es normalizada si su primera fila y columna tiene todos sus elementos iguales a uno.

Veamos entonces una condición necesaria que cumple toda matriz de Hadamard.

Teorema 3.11 *Sea H una matriz de Hadamard de orden n cuya primera fila tiene todas sus entradas iguales a 1. Entonces, el resto de filas de H tienen exactamente $\frac{n}{2}$ elementos iguales a 1 y $\frac{n}{2}$ elementos iguales a -1. Además, si $n > 2$, dos columnas cualesquiera de H tienen $\frac{n}{4}$ elementos iguales a 1 y -1 en común (sin tener en cuenta la primera fila).*

Demostración: Como hemos mencionado anteriormente, podemos definir una matriz de Hadamard como aquella matriz cuyas filas son ortogonales dos a dos, es decir, tal que el producto de dos filas cualesquiera es cero. Y por tanto, han de tener el mismo número de 1 que de -1; $\frac{n}{2}$.

Supongamos entonces que H es una matriz de Hadamard de orden $n > 2$ cuya primera fila tiene todas sus entradas iguales a 1.
Sean h_i y h_j dos filas cualesquiera de la matriz H, con $i \neq j$ y distintas de la primera. Entonces, denotaremos por u al número de columnas que tienen las filas h_i y h_j el elemento 1 en común y por v al número de columnas en las que aparece el elemento -1 en ambas filas a la vez. De este modo, habrá $(\frac{n}{2} - u)$ columnas en las que la fila h_i tenga el elemento 1 y la fila h_j tenga el elemento -1, y $(\frac{n}{2} - v)$ columnas en las que la fila h_j tenga el elemento 1 y la fila h_i tenga el elemento -1. Ahora, como cada fila de la matriz H ha de tener $\frac{n}{2}$ elementos iguales a 1, si tomamos la fila h_j obtenemos que $u + (\frac{n}{2} + v) = \frac{n}{2}$, es decir, $u = v$. Además, como ambas filas han de ser ortogonales entre sí, se cumple la siguiente ecuación:

$$0 = 1 \cdot 1u + 1(-1)(\frac{n}{2} - u) + (-1)(-1)v + (-1)1(\frac{n}{2} - v),$$

esto es, $u = \frac{n}{4}$. De esta forma podemos concluir que dos columnas cualesquiera de la matriz H tienen $\frac{n}{4}$ elementos iguales a 1 o a -1 en común. □

Como consecuencia directa de este teorema tenemos que si existe una matriz de Hadamard de orden n, entonces $n = 2$ o $n \equiv 0 \pmod 4$. Una forma de construir matrices de Hadamard de orden 2^n es de la siguiente manera:

$$H_1 = \begin{pmatrix}1\end{pmatrix}, \quad H_2 = \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad H_4 = \begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}, ..., \quad H_{2^n} = \begin{pmatrix}H_{2^{n-1}} & H_{2^{n-1}}\\ H_{2^{n-1}} & -H_{2^{n-1}}\end{pmatrix}$$

para todo $n \equiv 0 \pmod 4$.

Teorema 3.12 *Si H es una matriz de Hadamard de orden $4n$ con $n \geq 2$ entonces existe un $2-(4n-1, 2n-1, n-1)$ diseño, es decir, un diseño de Hadamard de orden n.*

Demostración: Sea H una matriz de Hadamard normalizada de orden $4n$ (podemos multiplicar cualquier fila y columna de la inicial por -1 para que lo sea). Si eliminamos la primera fila y columna de elementos iguales a 1, obtenemos una matriz H' de tamaño $(4n-1) \times (4n-1)$. Por el teorema 3.11, sabemos que cada fila de la matriz H tiene $\frac{4n}{2}$ elementos iguales a 1, luego la matriz H' tendrá $(\frac{4n}{2} - 1)$. Además, como el orden de la matriz es múltiplo de 4, sabemos que dos columnas cualesquiera de la matriz H tienen en común $\frac{4n}{4}$ elementos iguales a 1, luego en la matriz H' dos columnas tendrán $(\frac{4n}{4} - 1)$ elementos iguales a 1 en común.

De esta forma, si cambiamos las entradas de la matriz H' que son -1 por 0 e identificamos a las filas como bloques y las columnas como los elementos de un diseño, obtenemos que H' no es más que la matriz traspuesta de la matriz de indicencia de un $2-(4n-1, 2n-1, n-1)$ diseño. □

Veamos ahora que con la misma matriz de Hadamard podemos obtener también un 3−diseño.

Teorema 3.13 *Si H es una matriz de Hadamard de orden $4n$ con $n \geq 2$ entonces existe un $3-(4n, 2n, n-1)$ diseño.*

Demostración: Sea H una matriz de Hadamard de orden $4n$ con $n \geq 2$ cuya primera fila tiene todas sus entradas iguales a 1 (podemos multiplicar las columnas cuyo elemento de la primera fila no sea uno por -1 y la matriz seguirá siendo de Hadamard).
Los elementos del diseño serán las columnas de la matriz H y cada fila distinta de la primera formará dos bloques; uno estará formado por aquellas columnas que tengan un 1 en dicha fila y el otro estará formado por las columnas restantes, es decir, aquellas en las que aparezca un -1.

Está claro que el diseño estará formado por $4n$ elementos y que todos los bloques estarán formados por $\frac{4n}{2}$ elementos, ya que por el teorema 3.11 sabemos que toda fila de una matriz de Hadamard de orden $4n$ tiene la mitad de elementos iguales a 1 e iguales a -1. Así, basta ver que tres elementos cualesquiera del diseño aparecen juntos en exactamente $n-1$ bloques del diseño, es decir, que tres columnas cualesquiera de la matriz H tienen el elemento 1 o el elemento -1 a la vez en $n-1$ filas.

Tomemos h_{i_1}, h_{i_2} y h_{i_3} tres columnas cualesquiera de la matriz H, de modo que $\{h_{i_1}, h_{i_2}, h_{i_3}\} \in B_i$ si $h_{i_1} = h_{i_2} = h_{i_3} = 1$ o si $h_{i_1} = h_{i_2} = h_{i_3} = -1$. Denotaremos a los elementos de las filas de estas columnas como el vector $(h_{i_1}, h_{i_2}, h_{i_3})$ para simplificar la notación. Veamos entonces cuantas filas, excepto la primera, tienen $(1,1,1)$ y $(-1,-1,-1)$ en dichas columnas.

Como estamos trabajando con matrices de Hadamard, podemos multiplicar por -1 aquellas filas que tengan en esas posiciones $(-1,-1,-1)$ para conseguir $(1,1,1)$. De esta forma, la matriz seguirá siendo de Hadamard, los elementos de los bloques no cambiarán (pues intercambiamos los bloques de cada fila en la que esto ocurra) y solo tendremos que buscar las filas que tengan $(1,1,1)$ en dichas columnas. Además, por el mismo motivo, podemos hacer que todos los elementos de la columna h_{i_1} sean 1. Basta multiplicar todas las filas en las que aparezca el elemento -1 en esta columna. Del mismo modo, la matriz resultante seguirá siendo de Hadamard y los bloques estarán formados por los mismos elementos.

Supongamos ahora (con los cambios oportunos mencionados anteriormente) que en la matriz H hay a filas de la forma $(1,1,1)$, b filas de la forma $(1,1,-1)$, c filas de la forma $(1,-1,1)$ y d filas de la forma $(1,-1,-1)$:

	$(h_{i_1},$	$h_{i_2},$	$h_{i_3})$
a:	1	1	1
b:	1	1	-1
c:	1	-1	1
d:	1	-1	-1

Ahora, teniendo en cuenta que hay en total $4n$ filas y que en una matriz de Hadamard todas sus columnas son ortogonales dos a dos, obtenemos el siguiente sistema:

$$\begin{cases} a+b+c+d = 4n \\ a+b-c-d = 0 \\ a-b+c-d = 0 \\ a-b-c+d = 0 \end{cases} \tag{3.3}$$

La segunda, tercera y cuarta ecuación se obtienen por ser h_{i_1} y h_{i_2}, h_{i_1} y h_{i_3}, y h_{i_2} y h_{i_3} columnas ortogonales respectivamente.
Resolviendo este sistema (3.3) obtenemos que $a = n$, es decir, hay n filas de la forma $(1,1,1)$. Por lo

tanto, sin tener en cuenta la primera fila de la matriz, tenemos que hay $n-1$ filas de la forma $(1,1,1)$, como queríamos probar.

De este modo, si cambiamos los elementos iguales a -1 por 0 e identificamos las columnas de la matriz como elementos tal que cada fila distinta de la primera proporcione dos bloques; uno formado por todas las columnas en las que aparezca un 1 y otro formado por todas las columnas en las que aparezca un 0, obtenemos la matriz traspuesta de la matriz de incidencia de un $3-(4n,2n,n-1)$ diseño. □

Ejemplo 23 *Sea la siguiente matriz de Hadamard de orden* 8. *Si eliminamos de* H_8 *la primera fila y la primera columna y sustituimos los elementos* -1 *por* 0 *obtenemos la siguiente matriz* $H^{'}$*:*

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} \qquad H^{'} = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Si identificamos las columnas de la matriz $H^{'}$ *como elementos y las filas como bloques, obtenemos un diseño formado por el conjunto* $X = \{1,2,3,4,5,6,7\}$ *y el conjunto* B *formado por los bloques:*

$$\{2,4,6\}, \quad \{1,4,5\}, \quad \{3,4,7\}, \quad \{1,2,3\}, \quad \{2,5,7\}, \quad \{1,6,7\}, \quad y \quad \{3,5,6\}.$$

Es fácil ver que es un $2-(7,3,1)$ *diseño y que* $H^{'}$ *es la traspuesta de su matriz de incidencia.*

Si ahora directamente en la matriz H_8 *sustituimos los elementos* -1 *por* 0*, se obtiene la siguiente matriz* $H^{''}$*:*

$$H^{''} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Si identificamos las columnas de la matriz $H^{''}$ *como elementos y tomamos de cada fila (excepto la primera) dos bloques; uno formado por los índices de las columnas en los que aparece un* 1 *y otro formado por los elementos restantes, obtenemos un diseño formado por el conjunto* $X = \{1,2,3,4,5,6,7,8\}$ *y el conjunto* B *formado por los bloques:*

$$\begin{array}{lllllll} \{1,3,5,7\}, & \{2,4,6,8\}, & \{1,2,5,6\}, & \{3,4,7,8\}, & \{1,4,5,8\}, & \{2,3,6,7\}, & \{1,2,3,4\}, \\ \{5,6,7,8\}, & \{1,3,6,8\}, & \{2,4,5,7\}, & \{1,2,7,8\}, & \{3,4,5,6\}, & \{1,4,6,7\}, & \{2,3,5,8\}. \end{array}$$

Que claramente es un $3-(8,4,1)$ *diseño con* $H^{''}$ *la matriz traspuesta de su matriz de incidencia.*

3.3.2. Geometría afín

La última construcción que vamos a ver está basada en el conjunto de variedades afines de un espacio afín sobre un cuerpo finito.

Teorema 3.14 *Sea $\mathbb{A}^n(\mathbb{F}_q)$ un espacio afín de dimensión n sobre $\mathbb{F}_q$. El diseño formado por todos los puntos del espacio afín y por el conjunto de bloques formado por todas las variedades afines de dimensión m es un $2-(q^n, q^m, \left[\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right](q))$ diseño donde:*

$$\left[\begin{smallmatrix} h \\ k \end{smallmatrix}\right](x) = \frac{(x^h-1)(x^{h-1}-1)\cdots(x^{h-k+1}-1)}{(x^k-1)(x^{k-1}-1)\cdots(x-1)}.$$

Demostración: Sea $X = \mathbb{A}^n(\mathbb{F}_q)$ un espacio afín de dimensión n sobre $\mathbb{F}_q$. Como los elementos del diseño son todos los puntos del espacio afín, lógicamente se tiene que $|X| = |\mathbb{A}^n(\mathbb{F}_q)| = q^n$.
Veamos que cada bloque del diseño tiene q^m elementos, es decir, que cada variedad afín de dimensión m tiene q^m puntos. Sabemos que cada variedad afín $\mathcal{L}$ de dimensión m tiene las siguientes ecuaciones paramétricas:

$$\begin{aligned} x_1 &= p_1 + \alpha_1 v_1^1 + ... + \alpha_m v_1^m \\ x_2 &= p_2 + \alpha_1 v_2^1 + ... + \alpha_m v_2^m \\ &\vdots \\ x_n &= p_n + \alpha_1 v_n^1 + ... + \alpha_m v_n^m \end{aligned} \tag{3.4}$$

con $(p_1, p_2, ..., p_n) \in \mathbb{A}^n(\mathbb{F}_q)$ un punto cualquiera y $X_{\mathcal{L}} = \langle v_1, v_2, ..., v_m \rangle$ un subespacio vectorial de dimensión m. De este modo, tomando todos los valores posibles para $\alpha_1, \alpha_2, ..., \alpha_m$ obtenemos todos los puntos de la variedad, es decir,

$$|\mathcal{L}| = |\{(\alpha_1, \alpha_2, ..., \alpha_m) : \alpha_i \in \mathbb{F}_q\}| = q^m.$$

Y por tanto, todo bloque del diseño contiene q^m elementos.

Falta ver entonces que es un $2-$diseño con $\lambda = \left[\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right](q)$. Para ello hay que probar que dados $P, Q \in X$ dos puntos distintos, existen λ variedades afines de dimensión m que los contienen, independientemente de P y de Q. Sean $P, Q \in X$ dos puntos distintos. Sabemos que una variedad afín $\mathcal{L}$ de dimensión m queda unívocamente determinada por un punto y una dirección vectorial, $\mathcal{L} = R + V_{\mathcal{L}}$, la cual estará formada por m vectores independientes.
Como en un espacio afín podemos tomar cualquier punto como el origen, tomemos el punto P como tal. Así, las ecuaciones implícitas de todas las variedades de dimensión m que pasen por el punto P serán de la forma:

$$\begin{aligned} a_1^1 x_1 + a_2^1 x_2 + ... + a_n^1 x_n &= 0 \\ a_1^2 x_1 + a_2^2 x_2 + ... + a_n^2 x_n &= 0 \\ &\vdots \\ a_1^{n-m} x_1 + a_2^{n-m} x_2 + ... + a_n^{n-m} x_n &= 0 \end{aligned} \tag{3.5}$$

Además estas ecuaciones, al estar igualadas a cero, también representan el espacio vectorial asociado a esa variedad. En consecuencia, las variedades afines de dimensión m que contienen a los puntos $P = O = (0, 0, ..., 0)$ y a Q, es decir, aquellas variedades que tengan como ecuaciones implícitas (3.5) y que pasen por el punto Q, coinciden con los subespacios vectoriales de dimensión m que contienen al vector $\overrightarrow{PQ} = \overrightarrow{OQ}$.
Sea $V = \mathbb{F}_q^n$. Consideremos la aplicación $f : V \longrightarrow V/\langle \overrightarrow{PQ} \rangle$ de paso al cociente que se define a través de la siguiente relación de equivalencia en V:

$$v_1 \backsim v_2 \Longleftrightarrow v_1 - v_2 \in \langle \overrightarrow{PQ} \rangle.$$

con $dim(V/\langle \overrightarrow{PQ} \rangle) = n-1$.
Veamos que esta define una biyección $\bar{f}$ entre los subespacios vectoriales de dimensión m de V que contienen a $\overrightarrow{PQ}$ y los subespacios vectoriales de dimensión $(m-1)$ del espacio vectorial $V/\langle \overrightarrow{PQ} \rangle$:

- $\bar{f}$ bien definida: Sea W un subespacio de V tal que $\overrightarrow{PQ} \in W$. Queremos ver que si W es un subespacio vectorial de dimensión m que contiene a $\overrightarrow{PQ}$ entonces $\bar{f}(W)$ es un subespacio de dimensión $(m-1)$ de $V/\langle \overrightarrow{PQ} \rangle$. Para ello, basta considerar la base $W = \langle \overrightarrow{PQ}, w_1, ..., w_{m-1} \rangle$. Por ser vectores linealmente independientes, se tiene que $\bar{f}(W) = \langle [w_1], ..., [w_{m-1}] \rangle$. De lo contrario, si los vectores $[w_1], ..., [w_{m-1}]$ no fueran linealmente independientes, existirían $\alpha_1, \alpha_2, ..., \alpha_{m-1}$ para algún α_i no nulo tal que $\alpha_1[w_1] + \alpha_2[w_2] + \cdots + \alpha_{m-1}[w_{m-1}] = 0$, lo que implica que

  $$\alpha \overrightarrow{PQ} + \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_{m-1} w_{m-1} = 0.$$

  Ya que las clases $[w_i]$ son los vectores de la forma $w_i + k\overrightarrow{PQ}$. Y esto es absurdo porque suponíamos que W tenía dimensión m, es decir, su base estaba formada por vectores linealmente independientes entre sí.

- $\bar{f}$ sobreyectiva: sea W un subespacio de dimensión $(m-1)$ de $V/\langle \overrightarrow{PQ} \rangle$ generado por la siguiente base $\{[v_1], [v_2], ..., [v_{m-1}]\}$. Queremos ver que $\{\overrightarrow{PQ}, [v_1], [v_2], ..., [v_{m-1}]\}$ será la base de un subespacio vectorial de dimensión m de V que contiene al vector $\overrightarrow{PQ}$. Está claro que contiene a dicho vector, luego falta ver que tiene dimensión m. Sabemos que $[v_1], [v_2], ..., [v_{m-1}]$ son vectores independientes en $V/\langle \overrightarrow{PQ} \rangle$, veamos entonces que $\overrightarrow{PQ}$ es independiente a dichos vectores. Supongamos que no lo sea, es decir, que $\overrightarrow{PQ} = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{m-1} v_{m-1}$ para algún $\alpha_i \neq 0$, entonces se tiene que

  $$0 = \bar{f}(\overrightarrow{PQ}) = \alpha_1 \bar{f}(v_1) + \alpha_2 \bar{f}(v_2) + \cdots + \alpha_{m-1} \bar{f}(v_{m-1}) = \alpha_1[v_1] + \alpha_2[v_2] + \cdots + \alpha_{m-1}[v_{m-1}],$$

  y esto es absurdo ya que $\{[v_1], [v_2], ..., [v_{m-1}]\}$ era una base.

- $\bar{f}$ inyectiva: sean $W_1 = \langle \overrightarrow{PQ}, w_1^1, ..., w_{m-1}^1 \rangle$ y $W_2 = \langle \overrightarrow{PQ}, w_1^2, ..., w_{m-1}^2 \rangle$ dos subespacios distintos de V tales que $\overrightarrow{PQ} \in W_1$ y $\overrightarrow{PQ} \in W_2$. Claramente $\bar{f}(W_1)$ y $\bar{f}(W_2)$ son subespacios vectoriales de dimensión $(m-1)$ de $V/\langle \overrightarrow{PQ} \rangle$.
  Como $W_1 \neq W_2$, existe un vector de la base de W_1 que no pertenece a W_2. Supongamos que es w_1^1, entonces $[w_1^1] \in f(W_1)$ pero $[w_1^1] \notin f(W_2)$. Ahora supongamos lo contrario. Si $[w_1^1] \in f(W_2)$ tendríamos que $[w_1^1] = \lambda_1[w_1^2] + \cdots + \lambda_{m-1}[w_{m-1}^2]$, es decir,

  $$w_1^1 + k' \overrightarrow{PQ} = k\overrightarrow{PQ} + \lambda_1 w_1^2 + \cdots + \lambda_{m-1} w_{m-1}^2 \Longrightarrow w_1^1 = h\overrightarrow{PQ} + \lambda_1 w_1^2 + \cdots + \lambda_{m-1} w_{m-1}^2.$$

  Que es absurdo porque el vector w_1^1 no pertenecía al subespacio W_2.

Por lo tanto, vamos a determinar el número de subespacios vectoriales de dimensión $(m-1)$ del espacio vectorial $V/\langle \overrightarrow{PQ} \rangle$ (dimensión $n-1$).

Sea $W \subseteq V/\langle \overrightarrow{PQ} \rangle$ un subespacio vectorial de dimensión $(m-1)$, este queda determinado por la base de vectores independientes $w_1, w_2, ..., w_{m-1}$. Veamos de cuántas formas podemos elegir esos vectores. Como es un espacio vectorial de dimensión $(n-1)$, hay $(q^{n-1}-1)$ opciones de elegir el vector w_1, ya que no podemos tomar el vector nulo, $(q^{n-1}-q)$ opciones para el vector w_2, ya que no podemos tomar ningún múltiplo del vector w_1,$(q^{n-1}-q^2)$ opciones para el vector w_3, ya que no podemos tomar ningún múltiplo

del vector w_1 ni del vector w_2,..., y así sucesivamente, obtenemos que hay $(q^{n-1} - q^{m-2})$ opciones de elegir el vector w_{m-1}. Por lo tanto, en total hay $(q^{n-1}-1)(q^{n-1}-q)(q^{n-1}-q^2)\cdots(q^{n-1}-q^{m-2})$ opciones de tomar esos vectores independientes.
Hemos de tener en cuenta que varias bases distintas pueden generar el mismo subespacio vectorial. Así, como en W hay q^{m-1} vectores en total, habrá $(q^{m-1}-1)(q^{m-1}-q)(q^{m-1}-q^2)\cdots(q^{m-1}-q^{m-2})$ bases que den el mismo subespacio. Basta seguir el procedimiento anterior para seleccionar las posibles opciones para los vectores de esta base.
Por tanto, hay

$$\frac{(q^{n-1}-1)(q^{n-1}-q)(q^{n-1}-q^2)\cdots(q^{n-1}-q^{m-2})}{(q^{m-1}-1)(q^{m-1}-q)(q^{m-1}-q^2)\cdots(q^{m-1}-q^{m-2})} = \left[\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right](q)$$

subespacios vectoriales de dimensión $(m-1)$ del espacio vectorial $V/\langle\overrightarrow{PQ}\rangle$ o, lo que es lo mismo, subespacios vectoriales de dimensión m que contienen al vector $\overrightarrow{PQ}$. Y equivalentemente, es el número de variedades afines de dimensión m que contienen a los puntos P y Q.

Podemos concluir entonces que dos elementos cualesquiera del conjunto X pertenecen al mismo número de bloques del diseño; $\lambda = \left[\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right](q)$. Obteniendo así un $2-(q^n, q^m, \left[\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right](q))$ diseño. □

En particular, si tomamos $q = 2$ se cumple que además de ser un $2-(2^n, 2^m, \left[\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right](2))$ diseño, es un $3-(2^n, 2^m, \left[\begin{smallmatrix} n-2 \\ m-2 \end{smallmatrix}\right](2))$ diseño.

Teorema 3.15 *Sea $\mathbb{A}^n(\mathbb{F}_2)$ un espacio afín de dimensión n sobre $\mathbb{F}_2$. El diseño formado por todos los puntos del espacio afín y por el conjunto de bloques formado por todas las variedades afines de dimensión m es un $3-(2^n, 2^m, \left[\begin{smallmatrix} n-2 \\ m-2 \end{smallmatrix}\right](2))$ diseño.*

Demostración: Sea $X = \mathbb{A}^n(\mathbb{F}_2)$ un espacio afín de dimensión n sobre $\mathbb{F}_2$. Por el teorema 3.14 sabemos que el diseño tiene 2^n elementos, que cada bloque contiene a 2^m elementos y que dos elementos cualesquiera del conjunto pertenecen exactamente a $\left[\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right](2)$ bloques. Vamos a ver que además, tres elementos cualesquiera del conjunto pertenecen al mismo número de bloques.

Sean P, Q y R tres puntos distintos del espacio afín X y supongamos que el punto P es el origen. De este modo, queremos conocer el número de variedades afines de dimensión m que pasan por el origen y que contienen a P y a Q. Siguiendo el mismo procedimiento que en la demostración del teorema 3.14 anterior, eso equivale a ver el número de subespacios vectoriales de dimensión m que contienen a los vectores $\overrightarrow{PQ}$ y $\overrightarrow{PR}$ (o $\overrightarrow{PQ}$ y $\overrightarrow{QR}$). Cabe destacar que esos vectores son siempre linealmente independientes. Si no lo fueran, existiria $\mu \in \mathbb{F}_2$ tal que $\overrightarrow{PQ} = \mu\overrightarrow{PR}$. En ese caso, si $\mu = 0$ se tendría que $\overrightarrow{PQ} = 0$, es decir, $P = Q$, y si $\mu = 1$ se tendría que $\overrightarrow{PQ} = \overrightarrow{PR}$, es decir, $Q = R$. Llegando a un absurdo en ambos casos.
Por lo tanto, tenemos que ver cuántos subespacios vectoriales hay de dimensión m que contengan a esos dos vectores linealmente independientes. De nuevo, si definimos la aplicación $f : V \longrightarrow V/\langle\overrightarrow{PQ}, \overrightarrow{PR}\rangle$ de paso al cociente con $dim(V/\langle\overrightarrow{PQ}, \overrightarrow{PR}\rangle) = n-2$, el número de subespacios vectoriales de dimensión m en V que contengan a dichos vectores será igual al número de subespacios de dimensión $(m-2)$ que hay en el espacio vectorial de dimensión $(n-2)$, es decir, $\left[\begin{smallmatrix} n-2 \\ m-2 \end{smallmatrix}\right](2)$.

Podemos concluir entonces que tres elementos cualesquiera del conjunto X pertenecen al mismo número de bloques del diseño; $\lambda = \left[\begin{smallmatrix} n-2 \\ m-2 \end{smallmatrix}\right](2)$. Obteniendo así un $3-(2^n, 2^m, \left[\begin{smallmatrix} n-2 \\ m-2 \end{smallmatrix}\right](2))$ diseño. □

Ejemplo 24 *Sea* $\mathbb{A}^3(\mathbb{F}_3)$ *un espacio afín de dimensión tres sobre* $\mathbb{F}_3$*. Vamos a ver que identificando los puntos de dicho espacio afín como elementos y las variedades afines de dimensión dos, es decir, los planos, como bloques, obtenemos un* $2-(27,9,4)$ *diseño.*

Por un lado, los puntos de $\mathbb{F}_3$ *son de la forma* (α,β,γ) *con* $\alpha,\beta,\gamma\in\{0,1,2\}$*.*

Ahora, las variedades afines de dimensión 2*, es decir, los planos del espacio afín* $\mathbb{A}^3(\mathbb{F}_3)$*, son de la forma*

$$\eta_1x+\eta_2y+\eta_3z=\theta$$

para $\eta_1,\eta_2,\eta_3,\theta\in\{0,1,2\}$ *elementos no todos nulos. De este modo, los planos* $\eta_1x+\eta_2y+\eta_3z=\theta$ *y* $\eta_1^{'}x+\eta_2^{'}y+\eta_3^{'}z=\theta^{'}$ *serán iguales sí, y solo sí,* $\frac{\eta_1}{\eta_1^{'}}=\frac{\eta_2}{\eta_2^{'}}=\frac{\eta_3}{\eta_3^{'}}=\frac{\theta}{\theta^{'}}$*.*

Identificando los puntos del espacio afín como elementos y los planos como bloques, se cumple que cada plano tiene 9 *puntos, es decir, cada bloque está formado por* 9 *elementos y que cada par de puntos están contenidos exactamente por* 4 *planos, es decir, que todo par de elementos pertenece al mismo número de bloques;* 4*. Por ejemplo, los planos* $x+2y+z=1$ *y* $2x+y=0$ *forman los bloques*

$$\begin{array}{cc} & \{(0,0,1),(1,0,0),(0,1,2),(2,1,0),(1,1,1),(2,0,2),(1,2,2),(2,2,1),(0,2,0)\}\\ y & \{(0,0,1),(0,0,2),(1,1,0),(1,1,1),(2,2,0),(2,2,2),(1,1,2),(2,2,1),(0,0,0)\}\end{array}$$

respectivamente, y los puntos $(0,0,1)$ *y* $(2,2,1)$ *están contenidos exactamente por los planos* $x+2y+z=1$*,* $2x+y=0$*,* $2x+y+z=1$ *y* $z=1$*, es decir, pertenecen a los bloques anteriores y a los siguientes:*

$$\begin{array}{cc} & \{(0,0,1),(0,1,0),(2,0,0),(1,0,2),(1,2,0),(1,1,1),(0,2,2),(2,1,1),(2,2,1)\}\\ y & \{(0,0,1),(0,2,1),(2,0,1),(0,1,1),(1,0,1),(1,1,1),(2,1,1),(1,2,1),(2,2,1)\}\end{array}$$

Sustituyendo los valores de los parámetros n,q *y* m *obtenemos, aplicando el teorema 3.14, un* $2-(27,9,4)$ *diseño.*

Bibliografía

[1] I. Anderson. *Combinatorial designs and Tournaments*. Oxford lectures series in mathematics and its applications, 6. Clarendon Press Oxford. 1998.

[2] I. Anderson y I. Honkala. *A short course in Combinatorial Designs*. Internet Edition, Spring, 1997.

[3] N. L. Biggs. *Matemática discreta*. Vicens Vives, 2002.

[4] R. C. Bose. *A Note on the Resolvability of Balanced Incomplete Block Designs*. Sankhyā: The Indial Journal of Statictics (1933-1960), 1942, vol. VI, Nº 2.

[5] R. C. Bose. *On the construction of balanced incomplete block designs*, Ann. Eugenics 9. 1939.

[6] A. Cayley. *On the triadic arrangements of seven and fifteen things*. Phil. Mag. 37. 1850; también en *The Collected Mathematical Papers of Arthur Cayley*, vol I. Cambridge University Press, Cambridge, 1889.

[7] C. J. Colbourn y J. H. Divitz. *Handbook of Combinatorial design*. Second edition. Discrete mathematics and its applications. Chapman & Hall/Taylor & Francis. 2007.

[8] F. N. Cole. *Kirkman parades*, Bull. Amer. Math. 28. 1922. págs. 435-437.

[9] F. Comellas, J. Fábrega, A. Sanchez y O. Serra. Matemática discreta. Edicions UPC. 2001.

[10] C. I. Cortés Pérez. *Propiedades y Aplicaciones de los Cuadrados Latinos*. Tesis de Maestria. Universidad Autónoma Metropolitana. 2011. <`http://mat.izt.uam.mx/mcmai/documentos/tesis/Gen.08-O/Cortes-CI-Tesis.pdf`>

[11] F. Cretté de Palluel. *Sur les avantages et l'économie que procurent les racines employées à l'engrais les moutons à l'étable*, Mémories d'Agriculture 14 (1788). págs. 17-23.

[12] L. Euler. *De cuadratis magicis* Euler Archive - All works (1849). 795. <`https://scholarlycommons.pacific.edu/euler-works/795`>. Fecha de último acceso: 1 de junio de 2021.

[13] L. Euler. *Recherches sur une nouvelle espèce de quarrés magiques*. Verh. Zeeuw. Gen. Weten. Vlissengen 9. 1782.

[14] R. A. Fisher. *An examination of the different possible solutions of a problem in incomplete blocks*.

[15] R. A. Fisher y F. Yates. *Statistical Tables for Biological, Agricultural and Medical Research*. Oliver and Boyd, Edinburgh, 1938.

[16] K. Ireland y M. Rosen. *A classical Introduction to Modern Number theory*. Second edition. Springer-Verlag. 1990.

[17] T. P. Kirkman. *On a problem in combinations.* Cambrigde and Dublin Math. J.2. 1847. págs. 191-204.

[18] T. P. Kirkman. *Note on an unanswered prize question.* Cambridge and Dublin Math. J.5. 1850. págs. 255-262.

[19] R. Lidl y H. Niederreiter, Finite Fields. Cambridge University Press. 1997

[20] D. K. Ray- Chaudhuri y R. M. Wilson. *On t-designs.* Osaka J. Math. 1975. págs. 737-744.

[21] J. Steiner. *Combinatorische Aufgabe*, J.Reine Angew. Math.45. 1853. págs. 181-182.

[22] D. R. Stinson. *Combinatorial Designs.* Springer, 2010.

[23] A. P. Street y D. J. Street. *Combinatorics of experimental Design.* Oxford University Press. 1987.

[24] W. D. Wallis. *Introduction to combinatorial designs*, Second edition. Discrete Mathematics and its applications. Chapmand & Hall/ CRC.

[25] W. S. B. Woolhouse. *Prize question 1733*, Lady's and Gentleman's Diary, 1844. pág. 84.

Apéndice A

Cuadrados latinos

Supongamos que queremos organizar un experimento de piscicultura agrícola para probar cinco nuevos tipos de piensos (A, B, C, D y E) en una granja acuática, de forma que si delimitamos la zona marítima en 25 piscinas iguales, cada pienso se aplique exactamente una vez en cada fila y en cada columna, con el objetivo de conocer, por ejemplo, la eficacia de la alimentación dependiendo de las condiciones en la que se encuentre cada piscina. Una posible solución a este problema sería el esquema siguiente:

A	B	C	D	E
B	C	A	E	D
C	D	E	A	B
D	E	B	C	A
E	A	D	B	C

Para resolver este tipo de problemas aparecen los cuadrados latinos, que han sido objeto de estudio durante años principalmente en el diseño de experimentos estadísticos.

Uno de los primeros ejemplos de cuadrados latinos en el diseño de experimentos fue introducido por Palluel [11] quién, en 1788, utilizó el siguiente cuadrado en un experimento con 16 ovejas de cuatro razas distintas. Es decir, con cuatro ovejas de cada raza.

1	2	3	4
4	1	2	3
3	4	1	2
2	3	4	1

Dicho problema consistía en organizar grupos de cuatro ovejas de forma que a cada grupo perteneciera una oveja de cada raza y tal que en cada raza hubiera cuatro dietas distintas. En este caso, si las razas se corresponden con las filas, las dietas con las columnas y cada número se corresponde con un día de la semana, entonces el cuadrado muestra la manera de seleccionar cuatro ovejas para sacrificar cada uno de los cuatro días, de modo que en cada día se sacrifique una oveja de cada raza y de cada dieta.

Sin embargo, fue Euler quién definió formalmente lo que se conoce hoy en día como cuadrados latinos en su manuscrito *"Recherches sur une nouvelle espece de quarre magique"*, en 1779. En particular, Euler estaba interesado en resolver el *"Problema de los 36 oficiales"* publicado en 1782, dando origen a los cuadrados latinos mutuamente ortogonales (dos cuadrados latinos A y B de orden n son ortogonales si todas las entradas en la unión de ambos (A, B) son distintas). Los oficiales fueron elegidos de modo que hubiera seis hombres de cada uno de los seis regimientos diferentes y que además, entre los seis oficiales de cada regimiento, hubiera un oficial de cada uno de los seis rangos distintos. Euler usaba el alfabeto griego para denotar los rangos y el alfabeto romano para denotar los regimientos, por este motivo,

denominaba greco-romanos a estos cuadrados. Este problema consistía en encontrar una formación de 6×6 oficiales de forma que en cada fila y en cada columna hubiese un oficial de cada regimiento y de cada rango.
Por lo tanto, este problema exige la existencia de dos cuadrados latinos de tal forma que superponiendo uno sobre el otro, se formen todas las posibles parejas, o dicho de otra forma, que no se repita ninguna.
Comencemos viendo un posible cuadrado en el que en cada fila y en cada columna aparezca solo un oficial de cada rango:

$$\begin{array}{cccccc} \alpha & \zeta & \beta & \epsilon & \gamma & \delta \\ \delta & \beta & \zeta & \gamma & \alpha & \epsilon \\ \beta & \epsilon & \gamma & \zeta & \delta & \alpha \\ \epsilon & \gamma & \alpha & \delta & \zeta & \beta \\ \zeta & \alpha & \delta & \beta & \epsilon & \gamma \\ \gamma & \delta & \epsilon & \alpha & \beta & \zeta \end{array}$$

Y ahora un posible cuadrado en el que en cada fila y en cada columna aprezca solo un oficial de cada regimiento:

$$\begin{array}{cccccc} \mathrm{A} & \mathrm{B} & \mathrm{C} & \mathrm{D} & \mathrm{E} & \mathrm{F} \\ \mathrm{C} & \mathrm{A} & \mathrm{B} & \mathrm{F} & \mathrm{D} & \mathrm{E} \\ \mathrm{B} & \mathrm{C} & \mathrm{A} & \mathrm{E} & \mathrm{F} & \mathrm{D} \\ \mathrm{D} & \mathrm{E} & \mathrm{F} & \mathrm{A} & \mathrm{B} & \mathrm{C} \\ \mathrm{F} & \mathrm{D} & \mathrm{E} & \mathrm{C} & \mathrm{A} & \mathrm{B} \\ \mathrm{E} & \mathrm{F} & \mathrm{D} & \mathrm{B} & \mathrm{C} & \mathrm{A} \end{array}$$

El problema tendrá solución si, superponiendo ambos cuadrados, cada pareja aparece una sola vez o ninguna se repite más de una vez.

$$\begin{array}{cccccc} \mathrm{A}\alpha & \mathrm{B}\zeta & \mathrm{C}\beta & \mathrm{D}\epsilon & \mathrm{E}\gamma & \mathrm{F}\delta \\ \mathrm{C}\delta & \mathrm{A}\beta & \mathrm{B}\zeta & \mathrm{F}\gamma & \mathrm{D}\alpha & \mathrm{E}\epsilon \\ \mathrm{B}\beta & \mathrm{C}\epsilon & \mathrm{A}\gamma & \mathrm{E}\zeta & \mathrm{F}\delta & \mathrm{D}\alpha \\ \mathrm{D}\epsilon & \mathrm{E}\gamma & \mathrm{F}\alpha & \mathrm{A}\delta & \mathrm{B}\zeta & \mathrm{C}\beta \\ \mathrm{F}\zeta & \mathrm{D}\alpha & \mathrm{E}\delta & \mathrm{C}\beta & \mathrm{A}\epsilon & \mathrm{B}\gamma \\ \mathrm{E}\gamma & \mathrm{F}\delta & \mathrm{D}\epsilon & \mathrm{B}\alpha & \mathrm{C}\beta & \mathrm{A}\zeta \end{array}$$

En este caso observamos que por ejemplo, la pareja $\mathrm{B}\zeta$ ó la pareja $\mathrm{C}\beta$ aparecen en más de una ocasión y sin embargo, la pareja $\mathrm{C}\gamma$ o la pareja $\mathrm{D}\delta$, entre otras, no aparecen en el cuadrado greco-latino. Euler conjeturó que no existía solución a este problema, y en general, conjeturó que para $n \equiv 2 \pmod 4$ no existía ningún cuadrado greco-latino de orden n. Años más tarde se probó que se podían construir cuadrados latinos ortogonales de cualquier orden excepto de tamaño $n = 2$ y $n = 6$.

Por ejemplo, para $n = 3$, podemos considerar un ejemplo clásico introducido por Fisher, en 1926. Este recuperó y utilizó de forma sistemática los cuadrados latinos para tratar esencialmente experimentos sobre la agricultura. En su ejemplo trataba de estudiar la incidencia conjunta de tres fertilizantes $\{f_1, f_2, f_3\}$ y tres insecticidas $\{i_1, i_2, i_3\}$ sobre un campo dividido en tres parcelas $\{A, B, C\}$, durante tres años consecutivos $\{1, 2, 3\}$. Para ello, es necesario combinar en cada año y en cada parcela una pareja formada por un fertilizante y un insecticida de forma que todas las parejas hayan sido probadas. Los siguientes cuadrados latinos muestran la solución a este problema:

$$\begin{array}{ccc} f_1 & f_2 & f_3 \\ f_2 & f_3 & f_1 \\ f_3 & f_1 & f_2 \end{array} \qquad \begin{array}{ccc} i_1 & i_2 & i_3 \\ i_3 & i_1 & i_2 \\ i_2 & i_3 & i_1 \end{array}$$

Si ahora superponemos ambos cuadrados:

	1	2	3
A	$f_1\ i_1$	$f_2\ i_2$	$f_3\ i_3$
B	$f_2\ i_3$	$f_3\ i_1$	$f_1\ i_2$
C	$f_3\ i_2$	$f_1\ i_3$	$f_2\ i_1$

Obtenemos todas las posibles combinaciones de fertilizantes con insecticidas, es decir, todas las parejas pueden ser probadas y, por lo tanto, existen dos cuadrados latinos ortogonales de tamaño tres que satisfacen el problema inicial.

Definición A.1 *Un cuadrado latino de orden n es una matriz de tamaño $n \times n$ cuyos términos pertenecen a un conjunto finito S de cardinal n, de manera que cada uno de los elementos aparece exactamente una vez en cada fila y en cada columna.*

En otras palabras, cada fila y cada columna de un cuadrado latino es una permutación de los elementos de S.

Ejemplo 25 *La matriz*

$$\begin{matrix} 1 & 2 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \end{matrix}$$

es un cuadrado latino de orden 4.

Definición A.2 *Sea L un cuadrado latino de orden n y sea el conjunto $S = \{1, 2, ..., n\}$. Denotaremos por $L(i, j)$ para todo $1 \leq i, j \leq n$ al elemento correspondiente a la fila i y columna j del cuadrado latino L. Con esto, se dice que*

- *L es conmutativo si $L(i, j) = L(j, i)$ para todo $1 \leq i, j \leq n$.*
- *L es idempotente si $L(i, i) = i$ para todo $1 \leq i \leq n$.*
- *L es normalizado si $L(i, 1) = i$ para todo $1 \leq i \leq n$.*

Lógicamente, un cuadrado latino idempotente no será normalizado y viceversa. Si nos fijamos en el cuadrado latino del ejemplo 25 observamos que es normalizado pero no es ni idempotente ni comnutativo. Un ejemplo de un cuadrado latino idempotente y conmutativo podría ser el siguiente:

Ejemplo 26 *La matriz*

$$\begin{matrix} 1 & 4 & 2 & 5 & 3 \\ 4 & 2 & 5 & 3 & 1 \\ 2 & 5 & 3 & 1 & 4 \\ 5 & 3 & 1 & 4 & 2 \\ 3 & 1 & 4 & 2 & 5 \end{matrix}$$

es un cuadrado latino de orden 5 *idempotente y conmutativo.*

Observación 1 *Un cuadrado latino L de orden par $n = 2k$ es semi-idempotente si $L(i, i) = i$ y $L(k + i, k + i) = i$ para todo $1 \leq i \leq k$.*

Es sencillo ver que existen cuadrados latinos de cualquier orden. Basta identificar el conjunto S con un grupo $G = \{g_1, ..., g_n\}$ del mismo orden y considerar como cuadrado latino $L^{'}$ la tabla de su operación. De tal manera que $L^{'}(i,j) = g_k$ sí, y solo sí, cumple que $g_k = g_i g_j$.

Teorema A.3 *Existe un cuadrado latino de orden n para cualquier entero positivo n.*

Demostración: Sea el conjunto $S = \{1, 2, ..., n\}$. Denotemos la primera fila del cuadrado con los elementos en el orden siguiente: $1, 2, 3, ..., n$. Ahora, para construir el resto de filas del cuadrado, basta con desplazar una posición de la fila anterior a la izquierda y los elementos desplazados y eliminados de la fila colocarlos en orden a continuación de esta. De esta forma, el cuadrado latino queda de la siguiente manera:

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & \cdots & \cdots & n \\ 2 & 3 & 4 & \cdots & \cdots & n & 1 \\ 3 & 4 & 5 & \cdots & n & 1 & 2 \\ \vdots & \vdots & \vdots & & & & \vdots \\ n & 1 & 2 & \cdots & \cdots & \cdots & n-1 \end{array}$$

Así, en cada fila y en cada columna aparece solo una vez cada elemento del conjunto S, y por tanto, es un cuadrado latino de orden n. □

Un ejemplo de este teorema es la tabla del grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ de los enteros módulo n.

El siguiente resultado nos va a permitir construir otros cuadrados latinos.

Teorema A.4 *Para cada $n \geq 2$, las matrices L y R de tamaño $n \times n$ definidas por*

$$L(i,j) = i + j \quad y \quad R(i,j) = i - j$$

para $i, j \in \mathbb{Z}/n\mathbb{Z}$, son cuadrados latinos.

Demostración: Comencemos viendo que la matriz L con entradas definidas como $L(i,j) = i + j$ para $i, j \in \mathbb{Z}/n\mathbb{Z}$ forma un cuadrado latino. Supongamos que dos elementos de la misma fila son el mismo, es decir, que los elementos de las posiciones (i,j) y $(i,j^{'})$ son el mismo. De esta forma,

$$i + j = L(i,j) = L(i,j^{'}) = i + j^{'} \tag{A.1}$$

Como el elemento $-i$ pertenece al conjunto $\mathbb{Z}/n\mathbb{Z}$, podemos añadirlo a ambos lados de la ecuación (A.1) y así $j = j^{'}$, lo que es absurdo. Por lo tanto, dado que hay n elementos y n filas, cada elemento aparecerá exactamente una vez en cada fila. Análogamente para las columnas. En consecuencia, la matriz L es un cuadrado latino.
Siguiendo el mismo procedimiento, podemos concluir que la matriz R definida por $R(i,j) = i - j$ también es un cuadrado latino. □

Corolario A.5 *Para todo $n \geq 2$, las matrices N y M de tamaño $n \times n$ cuyas entradas están definidas como $N(i,j) = j - i + 1 \pmod{n}$ y $M(i,j) = j + i - 1 \pmod{n}$ son cuadrados latinos.*

Los cuadrados latinos están estrechamente relacionados con la estructura de cuasigrupo de un conjunto.

Definición A.6 *Sea G un conjunto de cardinal n y sea $\circ$ una operación binaria definida en G, esto es, $\circ$: $G \times G \longrightarrow G$. Diremos que el par $(G, \circ)$ es un cuasigrupo de orden n si para todo $g_i, g_j \in G$ la ecuación $g_i \circ x = g_j$ tiene una única solución para $x \in G$, y la ecuación $y \circ g_i = g_j$ tiene una única solución para $y \in G$.*

Un cuadrado latino puede verse como la tabla de operaciones de un cuasigrupo. Por lo tanto, los cuadrados latinos y los cuasigrupos pueden verse como objetos combinatorios equivalentes y podremos usar estos dos términos indistintamente.

1	2	4	3
3	4	2	1
4	1	3	2
2	3	1	4

Cuadrado latino

$\circ$	1	2	3	4
1	1	2	4	3
2	3	4	2	1
3	4	1	3	2
4	2	3	1	4

Cuasigrupo

La tabla de operación de la operación binaria $\circ$ definida en G es la matriz A de tamaño $n \times n$ en la que cada elemento se define como $a_{x,y} = x \circ y$.

De la misma forma que en cuadrados latinos, se dice que un cuasigrupo $(G, \circ)$ de orden n es conmutativo si $x \circ y = y \circ x$ para todo $x, y \in G$ y se dice que es idempotente si $x \circ x = x$ para todo $x \in G$. Además, un cuasigrupo $(G, \circ)$ de orden $n = 2k$ será semi-idempotente si $i \circ i = i$ y $(k + i) \circ (k + i) = i$ para todo $1 \leq i \leq k$ con $i \in G$.

Teorema A.7 *Supongamos que G es un conjunto de cardinal n y sea $\circ$ una operación binaria definida en G. Entonces $(G, \circ)$ es un cuasigrupo sí, y solo sí, su tabla de operaciones es un cuadrado latino de orden n.*

Demostración: Comencemos viendo que es una condición necesaria. Sea $(G, \circ)$ un cuasigrupo y sean $\{g_1, ..., g_n\}$ los elementos de G. Definimos su tabla de operaciones de la siguiente forma:

$\circ$	g_1	g_2	$\cdots$	g_r	$\cdots$	g_s	$\cdots$	g_n
g_1	g_{11}	g_{12}		$\vdots$		$\vdots$		g_{1n}
g_2	g_{21}	g_{22}		$\vdots$		$\vdots$		g_{2n}
$\vdots$				$\vdots$		$\vdots$		$\vdots$
g_r	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	g_{rs}		
$\vdots$				$\vdots$				
g_s	$\cdots$	$\cdots$	$\cdots$	g_{sr}				
$\vdots$								$\vdots$
g_n	g_{n1}	g_{n2}	$\cdots$				$\cdots$	g_{nn}

Así, el elemento g_{rs} colocado en la fila r y en la columna s es el producto de $g_r \cdot g_s$.

Supongamos que en la fila r se repite un valor dos veces, esto es, $g_r \cdot g_s = g_r \cdot g_t = a$. Pero esto equivale a que la ecuación $g_r \cdot x = a$ posea dos soluciones distintas, y es absurdo ya que suponíamos que $(G, \circ)$ era un cuasigrupo. Por lo tanto, cada elemento de G aparece exactamente una vez en cada fila de la tabla de operaciones. Con el mismo procedimiento probamos que de igual forma, cada elemento de G aparece exactamente una vez en cada columna de la tabla de operaciones.
Así, la tabla de operaciones de $(G, \circ)$ es un cuadrado latino de orden n.

Veamos ahora que es condición suficiente. Supongamos que la tabla de operaciones del par $(G, \circ)$ es un cuadrado latino de orden n. Esto implica que cada elemento de G aparece solo una vez en cada fila y en cada columna de dicho cuadrado. Y, siguiendo la misma notación para definir los elementos de la tabla de cada fila y columna, esto equivale a decir que la ecuación $g_r \circ x = a$ y la ecuación $y \circ g_s = b$

tienen una única solución. Por tanto, $(G, \circ)$ es un cuasigrupo. □

A continuación, vamos a introducir los conceptos de isotopía e isomorfismo para cuasigrupos y cuadrados latinos.

Definición A.8 *Sean $(G, \circ)$ y $(H, *)$ dos cuasigrupos de orden n y sean θ, ϕ, ψ aplicaciones del conjunto G al conjunto H. Se dice que los cuasigrupos $(G, \circ)$ y $(H, *)$ son isotópicos si $\theta(x) * \phi(y) = \psi(x \circ y)$ para todo $x, y \in G$. A la tripleta ordenada (θ, ϕ, ψ) se la denomina isotopismo.*

Equivalentemente, el cuadrado latino L_2 será isótopo al cuadrado latino L_1 si sus filas, columnas y elementos son una permutación de las filas, columnas y elementos de L_1 respectivamente.

Ejemplo 27 *Consideremos el siguiente cuasigrupo $(G, \circ)$ con la tabla de operaciones:*

$\circ$	*1*	*2*	*3*	*4*
1	*1*	*2*	*3*	*4*
2	*2*	*3*	*4*	*1*
3	*3*	*4*	*1*	*2*
4	*4*	*1*	*2*	*3*

Supongamos que la aplicación ψ modifica los elementos del interior de la tabla de operaciones, la aplicación θ modifica los elementos de la primera columna y la aplicación ϕ los elementos de la primera fila. Si estas permutaciones son de la forma:

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad \phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

obtenemos que el cuasigrupo isotópico a $(G, \circ)$ respecto de las permutaciones ψ, θ, ϕ es:

$\circ$	*2*	*4*	*3*	*1*
3	*2*	*1*	*4*	*3*
2	*1*	*4*	*3*	*2*
4	*4*	*3*	*2*	*1*
1	*3*	*2*	*1*	*4*

De esta forma, si reescribimos este cuasigrupo de forma que la primera fila y la primera columna sigan el mismo orden que el cuasigrupo $(G, \circ)$, resulta que los siguientes cuasigrupos y cuadrados latinos correspondientes son isotópicos:

$\circ$	*1*	*2*	*3*	*4*
1	*1*	*2*	*3*	*4*
2	*2*	*3*	*4*	*1*
3	*3*	*4*	*1*	*2*
4	*4*	*1*	*2*	*3*

$\circ$	*1*	*2*	*3*	*4*
1	*4*	*3*	*1*	*2*
2	*2*	*1*	*3*	*4*
3	*3*	*2*	*4*	*1*
4	*1*	*4*	*2*	*3*

En particular, si el isotopismo (θ, ϕ, ψ) cumple que $\theta = \phi = \psi$, entonces es un isomorfismo. Para cuadrados latinos, diremos que un isomorfismo es un isotopismo que aplica la misma permutación a las filas, columnas y elementos. Podemos observar entonces que un isotopismo y un isomorfismo juegan un papel equivalente entre cuasigrupos y entre cuadrados latinos.

Una propiedad importante de los cuadrados latinos es la ortogonalidad, que surge cuando Euler en 1779 publica el *"Problema de los 36 oficiales"*. Definamos este concepto de forma más precisa.

Definición A.9 *Dos cuadrados latinos L_1 y L_2 de orden n son ortogonales si para cada par ordenado $(a,b) \in \{(1,1),(1,2),...,(n,n)\}$ existe exactamente una posición (i,j) para la cual $L_1(i,j) = a$ y $L_2(i,j) = b$. Lo denotaremos como $L_1 \perp L_2$.*

Tal y como se mencionó al introducir el *"Problema de los 36 oficiales"* de Euler, dos cuadrados latinos de orden n eran ortogonales si los n^2 pares ordenados son todos diferentes.

Ejemplo 28 *Los cuadrados latinos*

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{array}$$

$$\begin{array}{cccc} (1,1) & (2,2) & (3,3) & (4,4) \\ (3,4) & (4,3) & (1,2) & (2,1) \\ (4,2) & (3,1) & (2,4) & (1,3) \\ (2,3) & (1,4) & (4,1) & (3,2) \end{array}$$

son ortogonales. Cada uno de los 16 *pares ordenados* $\{(1,1),(1,2),...,(4,4)\}$ *aparece en una de las* 16 *posiciones. Sin embargo, los cuadrados latinos isótopos del ejemplo 27 no son ortogonales.*

El concepto de ortogonalidad se puede generalizar para un conjunto de cuadrados latinos. Se dice que una familia $L_1, L_2, ..., L_k$ de cuadrados latinos todos de orden n son mutuamente ortogonales si son ortogonales dos a dos. Para referirnos a un conjunto de cuadrados latinos mutuamente ortogonales se suele usar la abreviación *MOLS*.

Por último, vamos a ver un resultado que nos permite obtener cuadrados latinos y, en particular, ortogonales dos a dos.

Teorema A.10 *Sea $\mathbb{F}_p$ un cuerpo con p un número primo, entonces el cuadrado latino L_t definido por*

$$L_t = t \cdot i + j \tag{A.2}$$

para $t \in \mathbb{F}_p^*$ y $i, j \in \mathbb{F}_p$, es un cuadrado latino. Más aún, si $t \neq u$, los cuadrados latinos L_t y L_u son ortogonales.

Demostración: Sea $\mathbb{F}_p$ un cuerpo con p un número primo. Supongamos que dos elementos de la $i-$ésima fila son el mismo, es decir, que los elementos de las posiciones (i,j) y $(i,j^{'})$ son iguales. Siguiendo el mismo procedimiento que en el teorema A.4 obtenemos que es absurdo y que por tanto, cada elemento aparece exactamente una vez en cada fila. Veamos que pasa en el caso de las columnas. Supongamos ahora que los elementos de las posiciones (i,j) y $(i^{'},j)$ son iguales. Así,

$$ti + j = L_t(i,j) = L_t(i^{'},j) = ti^{'} + j \tag{A.3}$$

Por ser t elemento no nulo, es inversible en $\mathbb{F}_p^*$. Sumando el elemento $-j \in \mathbb{F}_p$ y multiplicando por t^{-1} en ambos lados de la ecuación se tiene $i = i^{'}$, que es absurdo. Podemos concluir entonces que L_t es un cuadrado latino, ya que cada elemento del conjunto $\mathbb{F}_p$ aparece exactamente una vez en cada fila y columna.

Veamos ahora que si tomamos los elementos $t, u \in \mathbb{F}_p^*$ distintos, L_t y L_u son cuadrados latinos ortogonales entre sí. Supongamos lo contrario, es decir, que existen dos posiciones distintas (i_1, j_1) y (i_2, j_2) tales que:

$$\begin{array}{ll} ti_1 + j_1 = k & ui_1 + j_1 = k^{'} \\ ti_2 + j_2 = k & ui_2 + j_2 = k^{'} \end{array} \tag{A.4}$$

es decir, que el par ordenado $(k, k^{'})$ aparece en dos posiciones distintas.
Operando dichas ecuaciones obtenemos que:

$$t(i_1 - i_2) = j_2 - j_1 \qquad u(i_1 - i_2) = j_2 - j_1 \tag{A.5}$$

Si $i_1 - i_2 = 0$, estas ecuaciones implican que $j_2 - j_1 = 0$ y, de esta forma, las posiciones (i_1, j_1) y (i_2, j_2) son la misma, que es absurdo. En consecuencia, $(i_1 - i_2)$ ha de ser distinto de cero y podemos resolver las ecuaciones (A.5), ya que posee inverso en $\mathbb{F}_p$. Así,

$$t = (i_1 - i_2)^{-1}(j_2 - j_1) = u \tag{A.6}$$

que es absurdo ya que suponiamos que $t \neq u$.
En consecuencia, los elementos k y $k^{'}$ solo pueden coincidir juntos exactamente en una única posición y por tanto los cuadrados latinos L_t y L_u son ortogonales. □

Para la realización de este Apéndice se han seguido las referencias [9], [10] y [23].